FRONTLINE TEST SYSTEM™

ETHERTEST

USER MANUAL

Copyright © 2000-2010 Frontline Test Equipment, Inc. All rights reserved. You may not reproduce, transmit, or store on magnetic media any part of this publication in any way without prior written authorization of Frontline Test Equipment, Inc.

FTS, Frontline and Frontline Test System are registered trademarks of Frontline Test Equipment, Inc. Frontline is a trademark of Frontline Test Equipment, Inc.

All other trademarks and registered trademarks are property of their respective owners.

Table of Contents

1 Welcome to FTS ____ *1*

2 Getting Started ____ *3*

2.1 Control Window ____ **3**

2.2 The Control Window Toolbar ____ **3**

2.3 Drop-Down Menus ____ **5**

2.4 Configuration Information on the Control Window ____ **5**

2.5 Status Information on the Control Window ____ **6**

2.6 Frame Information on the Control Window ____ **6**

2.7 Opening Ethertest ____ **7**

2.8 Minimizing Windows ____ **7**

3 Configuration Settings ____ *8*

3.1 Hardware Settings ____ **8**

3.1.1 Selecting an Ethernet Card ____ 8

3.2 Port Assignments ____ **8**

3.2.1 Adding or Changing Port Assignments ____ 8

3.3 Decoder Parameters ____ **9**

3.3.1 A2DP Decoder Parameters ____ 10

3.3.2 Security Parameters ____ 10

3.3.3 Decoder Parameter Templates ____ 11

3.4 Data Highway Plus Special Instructions for 1784-U2DHP ____ **12**

3.5 Ethernet ComProbe Special Instructions ____ **13**

3.5.1 Ethernet ComProbe Hardware Settings ____ 13

3.5.2 Ethernet ComProbe I/O Settings ____ 14

4 Protocol Stacks ____ *17*

4.1 Protocol Stack Wizard ____ **17**

4.2 Information Screen ____ **18**

4.3 Creating and Removing a Custom Stack ____ **18**

4.4 Saving User Defined Stacks ____ **19**

4.5 Reframing ____ **20**

4.6 Unframing ____ **21**

4.7 Providing Context For Decoding When Frame Information Is Missing ____ **21**

5 Capturing Data ____ *23*

5.1 Capturing Data ____ **23**

6 Analyzing Byte Level Data ____ *24*

6.1 Event Display ____ **24**

6.2 The Event Display Toolbar ____ **24**

6.3 Opening Multiple Event Display Windows ____ **26**

6.4 Calculating CRCs or FCSs ____ **26**

6.5 Calculating Delta Times and Data Rates ____ **27**

6.6 Switching Between Live Update and Review Mode ____ **28**

6.7 Data Formats and Symbols ____ **28**

6.7.1 Switching Between Viewing All Events and Viewing Data Events ____ 28
6.7.2 Switching Between Hex, Decimal, Octal or Binary ____ 28
6.7.3 Switching Between ASCII, EBCDIC, and Baudot ____ 29
6.7.4 Viewing Only ASCII (or EBCDIC or Baudot) ____ 29
6.7.5 Viewing Only Hex (Or Decimal or Octal or Binary) ____ 29
6.7.6 Selecting Mixed Channel/Sides ____ 30
6.7.7 List of All Event Symbols ____ 30
6.7.8 Font Size ____ 32

7 Analyzing Protocol Decodes ____ *33*

7.1 Frame Display Window ____ **33**

7.1.1 Frame Display Window ____ 33
7.1.2 Frame Display Toolbar ____ 34
7.1.3 Frame Display Status Bar ____ 37
7.1.4 Hiding and Revealing Protocol Layers in the Frame Display ____ 37
7.1.5 Physical vs. Logical Byte Display ____ 37
7.1.6 Sorting Frames ____ 38
7.1.7 Synchronizing the Event and Frame Displays ____ 38
7.1.8 Working With Multiple Frame Displays ____ 38
7.1.9 Working With Panes ____ 39
7.1.10 The Panes in the Frame Display ____ 39
7.1.11 Protocol Layer Colors ____ 45
7.1.12 Protocol Filtering from the Frame Display ____ 45

7.2 Protocol Navigator Window ____ **48**

7.2.1 Protocol Navigator ____ 48
7.2.2 Protocol Navigator Toolbar ____ 48
7.2.3 Protocol Navigator Status Bar ____ 50
7.2.4 The Difference Between Filtering and Hiding ____ 50
7.2.5 Hiding and Revealing Protocol Layers in the Protocol Navigator ____ 51
7.2.6 Filtering on a Protocol Layer ____ 51
7.2.7 Filtering on all Frames with Errors ____ 52
7.2.8 Expanding and Collapsing Protocol Layers ____ 52

8 Statistics ____ *55*

8.1 Statistics Window ____ **55**

8.2 Session, Resettable and Capture File Tabs ____ **55**

8.3 Copying Statistics To The Clipboard 56

8.4 Graphs 56

8.4.1 Statistics Graphs 56
8.4.2 Printing Graphs 56
8.4.3 Changing the Graph Refresh Rate 57
8.4.4 Viewing Percentages or Values 57

8.5 Information on Tables 57

8.5.1 Statistics Tables 57
8.5.2 Bytes Per Second Table 58
8.5.3 Frames Per Second Table 58
8.5.4 Utilization Table 58
8.5.5 Data Table 59
8.5.6 Unfiltered Data Table 60
8.5.7 Buffer Information Table 61
8.5.8 Errors Table 61

***9 Network View* 65**

9.1 Network View Introduction 65

9.2 Display Node Information in Network View 65

9.3 Displaying Conversation Information in Network View 67

9.4 Adding/Editing an Alias for a Node in Network View 68

9.5 Filter and Sort the Network View 68

9.6 Setting The Count For Top N Filters 70

9.7 Detail Window Layouts in Network View 70

9.8 The Statistics Graph Window in Network View 73

9.9 The Network View Node Database 73

9.10 Resolving DNS Names in Network View 74

9.11 The Network View Toolbar 74

9.12 Network View Visual Elements 75

9.13 Network View Technical Notes 76

9.14 Network View - Frame Sizes 80

***10 NetDecoder Dashboard* 81**

10.1 Dashboard 81

10.1.1 One Hour/Ten Minute Chart 82
10.1.2 Dashboard: Utilization (Percentage of Bandwidth) and Throughput (Percentage of Actual Traffic) 82
10.1.3 Top Talkers Bar Chart 83
10.1.4 Show DNS Names 83
10.1.5 Bandwidth Drop-down 84

10.1.6 Network Utilization Meter 84
10.1.7 Bad Packets Meter 84
10.1.8 % Top Utilization/Top Utilizer Meter 84
10.1.9 Charts 85
10.1.10 Network Alarms (Utilization) 85
10.1.11 App Distribution (Utilization/Throughput) 86
10.1.12 IP Addresses 86
10.1.13 Dashboard - Define Applications and Alarms 86
10.1.14 Define Email Addresses 88
10.1.15 Dashboard - Define Authorized IP Addresses 88
10.1.16 Dashboard - Show IP Addresses Seen 89

11 Find 91

11.1 Starting a Search 91

11.2 Using Go To 91

11.3 Searching for Frame Errors 93

11.4 Searching for Special Events 94

11.5 Searching within Decodes 95

11.6 Searching by Signal 96

11.7 Changing Where the Search Lands 96

11.8 Subtleties of Timestamp Searching 97

11.9 Entering Search Patterns (String Searches) 97
11.9.1 Searching by Pattern 97
11.9.2 Entering Characters 98
11.9.3 Entering Hex or Binary 98
11.9.4 Control Characters 98
11.9.5 Wildcard Character 99
11.9.6 Examples of Search Strings 99

11.10 Searching by Time 100
11.10.1 Searching by Time 100
11.10.2 Searching with Absolute Timestamp 101
11.10.3 Searching with Relative Timestamp 101
11.10.4 Choosing "On or Before" or "On or After" 102

12 Bookmarks 103

12.1 Bookmarks 103

12.2 Adding, Modifying or Deleting a Bookmark 103

12.3 Displaying All and Moving Between Bookmarks 104

13 Filtering 105

13.1 Difference Between Ethernet Capture Filters and Display Filters 105

13.2 Display Filters 105

13.2.1 About Display Filters 105
13.2.2 Including and Excluding Radio Buttons 106
13.2.3 Creating a Display Filter 106
13.2.4 Named Display Filters 107
13.2.5 Using Compound Display Filters 108
13.2.6 Defining Node and Conversation Filters 109
13.2.7 Using Advanced Display Filtering Techniques 109
13.2.8 Deleting and Hiding Display Filters 110
13.2.9 Editing Filters 111

13.3 Ethernet Capture Filters 112
13.3.1 Creating and Using an Ethernet Capture Filter 112
13.3.2 Applying an Ethernet Capture Filter 113
13.3.3 Removing an Ethernet Capture Filter 114
13.3.4 Defining Node and Conversation Ethernet Capture Filters 114
13.3.5 Selecting Predefined Ethernet Capture Filters 115
13.3.6 Defining Pattern or Offset Ethernet Capture Filters 115
13.3.7 Using BPF to Create a Custom Ethernet Capture Filter 115
13.3.8 Creating/Deleting a Compound Filter 116
13.3.9 Naming Ethernet Capture Filters 117
13.3.10 Modifying a Condition in an Ethernet Capture Filter 117
13.3.11 Deleting a Condition in an Ethernet Capture Filter 117
13.3.12 Filter Formats 118
13.3.13 Saving and Loading Capture Filter Files 124

13.4 Protocol Filtering from the Frame Display 125
13.4.1 Easy Protocol Filtering 125
13.4.2 Filtering On the Summary Layer Protocol 125
13.4.3 Quick Filtering on a Protocol Layer 125
13.4.4 Filtering on all Frames with Errors from the Frame Display 126

13.5 Protocol Filtering from the Protocol Navigator 126
13.5.1 Filtering on a Protocol Layer 126
13.5.2 Filtering on all Frames with Bookmarks 127
13.5.3 Filtering on all Frames with Errors from the Protocol Navigator 127
13.5.4 Filtering on all Frames with Special Information Nodes 127
13.5.5 Named Filters 127

14 Saving Data 129

14.1 Saving Your Data 129

14.2 Saving the Entire Capture File using File > Save or the Save icon 129

14.3 Saving the Entire Capture File with Save Selection 130

14.4 Saving a Portion of a Capture File 131

14.5 Confirm Capture File (CFA) Changes 132

14.6 Adding Comments to a Capture File 133

15 Loading and Importing Capture Files 135

15.1 Loading a Capture File 135
15.2 Importing Capture Files 135
15.3 Converting Timestamps 136
15.4 Adding Comments to a Capture File 136
15.5 File Format for Merlin Files 137
16 Printing ***139***
16.1 Printing from the Frame Display/HTML Export 139
16.2 Frame Display HTML Export 141
16.3 Printing from the Event Display 142
16.4 Print Preview 144
17 Exporting ***147***
17.1 Export 147
17.2 Export Filter Out 147
17.3 Exporting Event Display to a File 147
17.4 Exporting Baudot 149
17.5 HTML Export 149
18 System Settings and Program Options ***151***
18.1 System Settings 151
18.2 System Settings - Disabled/Enabled Options 153
18.3 Advanced System Options 153
18.4 Changing Default File Locations 154
18.5 Selecting Start Up Options 155
18.6 Timestamping 156
18.6.1 Timestamping Options 156
18.6.2 Enabling/Disabling Timestamping 156
18.6.3 Switching Between Relative and Absolute Time 156
18.6.4 Changing the Timestamping Resolution 157
18.6.5 Displaying Fractions of a Second 158
18.6.6 Converting Timestamps 158
18.6.7 Performance Issues For High Resolution Timestamps 158
19 Technical Information ***159***
19.1 Contacting Technical Support 159
19.2 Ethernet Performance Notes 159
19.3 Changing Where the Search Lands 160

19.4 Progress Bars 161
19.5 Event Numbering 161
19.6 Padding of Short Frames 161
19.7 CRC! 162
19.8 BPF Copyright Notice 162
19.9 Useful Character Tables 163
19.9.1 ASCII Codes 163
19.9.2 Baudot Codes 163
19.9.3 EBCDIC Codes 164
19.9.4 Communication Control Characters 164
19.10 Frame Decoder 166
20 Index ***167***

1 Welcome to FTS

Welcome to Frontline Test System (FTS). The design of FTS allows you to conduct data analysis of protocols using your personal computer. The FTS interface is easy to use without training, but we recommend you read the online Help to take maximum advantage of all the features.

We designed the online Help System with complete explanations and easy to use systematic instructions. Access the online Help by choosing Help Topics from the Help menu, or by pressing the F1 key on any window.

2 Getting Started

2.1 Control Window

The analyzer displays information in multiple windows, with each window presenting a different type of information. The *Control* window provides access to each window as well as a brief overview of the data in the capture file. Each icon on the toolbar represents a different data analysis function.

Because the *Control* window can get lost behind other windows, every window has a *Home* icon that brings the *Control* window back to the front. Just click on the *Home* icon to restore the *Control* window.

When running the *Capture File Viewer*, the *Control* window toolbar and menus contain only those selections needed to open a capture file and display the About box. Once a capture file is opened, the analyzer limits Control window functions to those that are useful for analyzing data contained in the current file. Because you cannot capture data while using *Capture File Viewer*, data capture functions are unavailable. For example, when viewing Ethernet data, the Signal Display is not available. The title bar of the Control window displays the name of the currently open file. The status line (below the toolbar) shows the configuration settings that were in use when the capture file was created.

2.2 The Control Window Toolbar

Available options are in color, while unavailable options are grayed out. All toolbar icons have corresponding menu items. Toolbar icon displays vary according to operating mode and/or data displayed.

Open File - Opens a capture file.

I/O Settings - Opens the I/O Settings dialog.

Start Capture - Begins data capture to disk.

Stop Capture - Available after data capture has started. Click to stop data capture. Data can be reviewed and saved, but no new data can be captured.

Clear - Clears or saves the capture file.

Event Display - (framed data only) Opens a Event Display, with the currently selected bytes highlighted.

Frame Display - (framed data only) Opens a Frame Display, with the frame of the currently selected bytes highlighted.

Protocol Navigator - (framed data only) Opens the Protocol Navigator window, with the currently selected frame highlighted.

Statistics Window - Opens up the Statistics window.

Signal Display - Opens The Signal Display dialog.

Breakout Box - Opens the Breakout Box dialog.

Transmit - Opens the Transmit dialog.

Cascade - Arranges windows in a cascaded display.

Packet Timeline - Opens the Packet Timeline display.

Extract Data - Opens the Extract Data dialog.

Packet Error Rate Statistics - Opens the Packet Error Rate Statistics window.

Audio Extraction - Opens the Audio Extraction dialog.

Network View - Opens the Network View Window.

Dashboard - Opens the Dashboard dialog

2.3 Drop-Down Menus

The menus that you see on the Control Window and dialogs like Frame Display and Event Display vary depending on whether the data is being captured live or whether you are looking at a .cfa file. You will see File, View, Live, Options, Window, and Help. Most of the options are self explanatory.

- Many of the **File** menu items are standard Windows type commands: Open, Close, Save, Recent Files, etc. There are two exceptions:
    - **Recreate Companion File**. This option is available when you are working with decoders. If you change a decoder while working with data, you can use Recreate Companion File to recreate the .frm file, the companion file to the .cfa file. Recreating the .frm file helps ensure that the decoders will work properly.
    - **Reload Decoders**. When Reload Decoders is clicked, the plug-ins are reset and received frames are redecoded.
- Under the **View** menu you can choose which FTS windows are available to open.
- **Live** contains commands that used in capturing data.
- Under **Options** you have opportunities to set/modify various system settings.
- The **Window** menu displays the open FTS dialogs and standard options like Cascade, Minimize, Tile, etc.
- Within the **Help** menu you can open the electronic Help file, About FTS, and access the FTS web site for additional help.

2.4 Configuration Information on the Control Window

The *Configuration* bar (just below the toolbar) displays the hardware configuration and may include I/O settings. It also provides such things as name of the network card, address information, ports in use, etc. If the analyzer cannot find the MAC Address, it lists zeroes after the NIC name.

2.5 Status Information on the Control Window

The *Status* bar located just below the *Configuration* bar on the *Control* window provides a quick look at current activity in the analyzer.

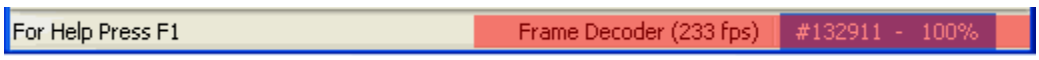
- *Capture Status* displays *Not Active*, *Paused* or *Running* and refers to the state of data capture.
    - *Not Active* means that the analyzer is not currently capturing data
    - *Paused* means that data capture has been suspended
    - *Running* means that the analyzer is actively capturing data.

- % Used
    - The next item shows how much of the buffer or capture file has been filled. For example, if you are capturing to disk and have specified a 200K capture file, the bar graph tells you how much of the capture file has been used. When the graph reaches 100%, capture either stops or the file begins to overwrite the oldest data, depending on the choices you made in the System Settings.

- Utilization/Events
    - The second half of the status bar gives the current utilization and total number of events seen on the network. This is the total number of events monitored, not the total number of events captured. The analyzer is always monitoring the circuit, even when data is not actively being captured. These graphs allow you to keep an eye on what is happening on the circuit, without requiring you to capture data.

2.6 Frame Information on the Control Window

Frame Decoder information is located just below the *Status* bar on the *Control* window. It displays two pieces of information.



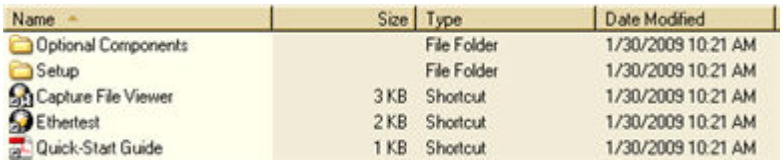
- **Frame Decoder (233 fps)** displays the number of frames per second being decoded. You can toggle this display on/off with Ctrl-D, but it is available only during a live capture.
- **#132911** displays the total frames decoded.
- **100%** displays the percentage of buffer space used.

2.7 Opening Ethertest

On product installation, the installer creates a folder on the windows desktop labeled **Ethertest**.

1. Double-click the Frontline Ethertest desktop folder.

This opens a standard Windows file folder window.



Name	Size	Type	Date Modified
Optional Components		File Folder	1/30/2009 10:21 AM
Setup		File Folder	1/30/2009 10:21 AM
Capture File Viewer	3 KB	Shortcut	1/30/2009 10:21 AM
Ethertest	2 KB	Shortcut	1/30/2009 10:21 AM
Quick-Start Guide	1 KB	Shortcut	1/30/2009 10:21 AM

2. Double-click on Ethertest and the application opens.

Note: You can also open the application by selecting *Start > All Programs > Frontline Ethertest (Version #) > Ethertest*.

2.8 Minimizing Windows

Windows can be minimized individually or as a group when the *Control* window is minimized.

To minimize windows as a group:

1. Go to the *Window* menu on the *Control* window
2. Select *Minimize Control Minimizes All*. The analyzer puts a check next to the menu item, indicating that when the Control window is minimized, all windows are minimized.
3. Select the menu item again to deactivate this feature.
4. The windows minimize to the top of the operating system Task Bar.

3 Configuration Settings

3.1 Hardware Settings

3.1.1 Selecting an Ethernet Card

The first time you start the NetDecoder Ethernet analyzer, the *Hardware Settings* dialog appears:

1. Select the Ethernet card the system should use
2. Click *OK*.

If you need to change your Ethernet card in the future, choose *Hardware Settings* from the *Options* menu on the Control window.

The analyzer checks the registry for Ethernet card entries and puts these in the drop-down list. On some PCs, the Ethernet Controller may be listed, or the Dial-Up Adapter. Be sure to choose the name of the NIC that is connected to the network.

Note: The Ethernet card must use an NDIS driver.

3.2 Port Assignments

3.2.1 Adding or Changing Port Assignments

The analyzer autotraverses the stack from TCP, UDP and IPX based on the source or destination port number. Many systems use user-defined port numbers for both standard and custom protocols. Here's how to tell the analyzer about a custom port assignment on the system you are monitoring.

Add a New Port Assignment

1. Choose *Set Initial Decoder Parameters* from the *Options* menu on the Control window.

2. Click the *TCP* tab (or UDP or IPX for those protocols).
3. Choose the *Single Port* radio button, and enter the port number in the *Port Number* box.
4. In the *Protocol* drop-down list, choose the protocol to traverse to.
5. Click the *Add* button. The system adds new entry to the bottom of the port number list.

Modify an Existing Port Assignment

1. Choose *Set Initial Decoder Parameters* from the *Options* menu on the Control window.
2. Click the *TCP* tab (or UDP or IPX for those protocols).
3. Select (click on and highlight) the port assignment to modify.
4. Change the port number and/or choose the protocol to traverse to.
5. Click the *Modify* button. The system displays the changes in port number list.
6. You can also specify a range of ports. Select the *Port Range* radio button and specify the starting and ending port numbers. The range is inclusive.
7. To remove an entry, select the entry and click *Delete*.

Two considerations are:

- The analyzer traverses an entry if either the source or destination port match
- The analyzer processes port number entries in order from top to bottom

If you need to move an entry to ensure it is processed before or after another entry, select the entry in the list and then click the *Move Up* or *Move Down* buttons.

3.3 Decoder Parameters

Some protocol decoders have user-defined parameters. These are protocols where some information cannot be discovered by looking at the data and must be entered by the user in order for the decoder to correctly decode the data. For example, such information might be a field where the length is either 3 or 4 bytes, and which length is being used is a system option.

If you have decoders loaded which require decoder parameters, a window with one tab for every decoder that requires parameters appears the first time the decoder is loaded.

For help on setting the parameters, click the Help button on each tab to get help information specific to that decoder.

If you need to change the parameters later,

- Choose Set Initial Decoder Parameters from the Options menu on the Control, Frame Display or Protocol Navigator windows.
- Each entry in the Set Initial Decoder Parameters dialog takes effect from the beginning of the capture onward or until redefined in the Set Subsequent Decoder Parameters dialog.

The Set Subsequent Decoder Parameters dialog allows the user to override an existing parameter at any frame in the capture where the parameter is used.

If you have a parameter in effect and wish to change that parameter

- Select the frame where the change should take effect
- Select Set Subsequent Decoder Parameters from the Options menu, and make the needed changes.
- Each entry in the Set Subsequent Decoder Parameters dialog takes effect from the specified frame onward or until redefined in this dialog on a later frame.

If you do not have decoders loaded that require parameters, the menu item does not appear and you don't need to worry about this feature.

3.3.1 A2DP Decoder Parameters

3.3.1.1 Selecting A2DP Decoder Parameters

The decoding of SBC frames in the A2DP decoder can be slow if the analyzer decodes all the parts (the header, the scale factor and the audio samples) of the frame in detail. You can increase the decoding speed by decoding only the header fields and not all the parts if they are not required. You can select the detail-level of decoding using the **Set Initial Decoder Parameters** dialog.

Note: By default the decoder decodes only the header fields of the frame.

1. Select *Set Initial Decoder Parameters* from the *Options* menu on the Control window, the Frame Display window, or the Protocol Navigator window to display the *Set Initial Decoder Parameters* dialog.
2. Click on the *A2DP* tab.
3. Choose the desired decoding method.
4. Click the *OK* button to apply the selection and exit the *Set Initial Decoder Parameters* dialog.

3.3.2 Security Parameters

3.3.2.1 Security Key

On the Set Initial Decoder Parameters dialog, the security tab allows specifying a key for software decryption of 802.11 frames. One can enter two types of keys. The types are a WPA (Wi-Fi Protected Access) pre-shared key and a WEP (Wired Equivalent Privacy) key.

To access this dialog:

1. Go to the *Options* menu on the Control window and choose *Set Initial Decoder Parameters.*
2. Select the *Security* tab.

There are three types of types of encrypted data on the security tab, each one selectable via a radio button.

- WPA, WPA2 (Wi-Fi Protected Access), and WEP (Wired Equivalent Privacy) data that is transmitted over a Wi-Fi communications link. There are two values you have to enter for the WPA/WPA2 and WEP to be decrypted properly.
- The Bluetooth® alternative MAC/PHY (AMP) enables Bluetooth to support data rates up to 24Mbps by using additional wireless radio technologies.
- The Pre-Shared Key: The third way is to specify the pre-shared key in its raw hex forum. This is a 32 byte hex number.
  Note: When you use WPA/WPA2, the Pre-Shared key is generated automatically.

Depending on which Encrypted Data type you select, the options for entering data on the rest of the dialog varies.

3.3.3 Decoder Parameter Templates

3.3.3.1 Adding a New or Saving an Existing Template

A template is a collection of parameters required to completely decode communications between multiple devices. This procedure adds a template to the system and saves it for later use:

1. Click the Save button at the top of the Set Initial Decoder Parameters dialog to display the Save As dialog.
2. Enter a name for the new template and click Ok.

The system saves the template and closes the Save As dialog.

3. Click the Ok button on the Set Initial Decoder Parameters dialog to apply the template and close the dialog.

Save Changes to a Template

This procedure saves changes to parameters in an existing template.

1. After making changes to parameter settings in a user defined template, click the Save button at the top of the Set Initial Decoder Parameters dialog to display the Save As dialog.
2. Ensure that the name of the template is listed in the Save As text box and click Ok.

The system displays a dialog asking for confirmation of the change to the existing template.

3. Click the Yes button.

The system saves the parameter changes to the template and closes the Save As dialog.

4. Click the Ok button on the Set Initial Decoder Parameters dialog to apply the template and close the dialog.

3.3.3.2 Deleting a Template

1. After opening the *Set Initial Decoder Parameters* dialog click the Delete button at the top of the dialog.

   The system displays the Delete dialog with a list of saved templates.

2. Select (click on and highlight) the template marked for deletion and click the Delete button on the Delete dialog.

   The system removes the selected template from the list of saved templates.

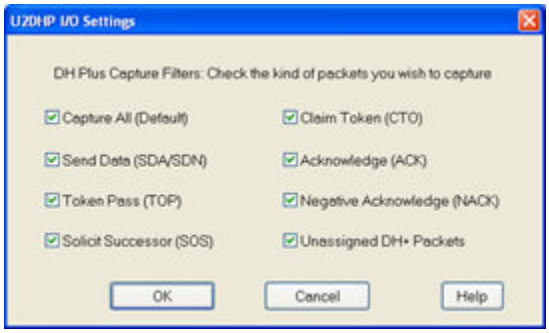
3. Click the Ok button on the Delete dialog to complete the deletion process and close the Delete dialog.
4. Click the Ok button on the Set Initial Decoder Parameters dialog to apply the deletion and close the dialog.

3.4 Data Highway Plus Special Instructions for 1784-U2DHP

3.4.1.1 DH Plus 1784-U2DHP I/O Settings

The DH Plus analyzer, using the 1784-U2DHP, allows users to select what type of packets are captured. This type of filtering eliminates capturing unnecessary frames and allows the user to quickly pin-point the source of the network problem. You select which frames to capture using the I/O settings dialog.

You access the I/O Settings dialog by selecting **IO Settings** from the **Options menu** on the NetDecoder Control window.



1. Select the kind of DH+ frames you need to capture by clicking the appropriate check boxes.

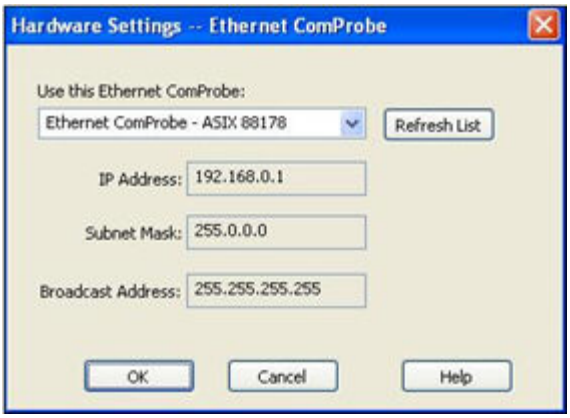
- If more than one box is checked, then the selection is treated as a logical AND condition.
- The default setting is to capture all traffic.
- If none of the items are checked on the dialog, the program defaults to a 'capture-all' state.

2. Select **OK** to accept the values and close the dialog or **Cancel** to disregard the settings and close the dialog.

3.5 Ethernet ComProbe Special Instructions

3.5.1 Ethernet ComProbe Hardware Settings

The Hardware Settings dialog allows you to select a specific Ethernet ComProbe device to sniff your Ethernet traffic.



1. You access the Hardware Settings dialog by selecting Hardware Settings from the Options menu on the NetDecoder Control window.
2. Select a **device** from the drop-down list

Note: FTS automatically scans and identifies all the Ethernet ComProbe devices plugged into the PC.

The IP address, subnet Mask and the Broadcast Address for that particular device are displayed.These are display only and cannot be edited.

3. If that is the right device you wish to use, select **OK**. Selecting Cancel overrides all the selections and returns the user to the Control Window.

There are a couple of things to remember about this dialog.

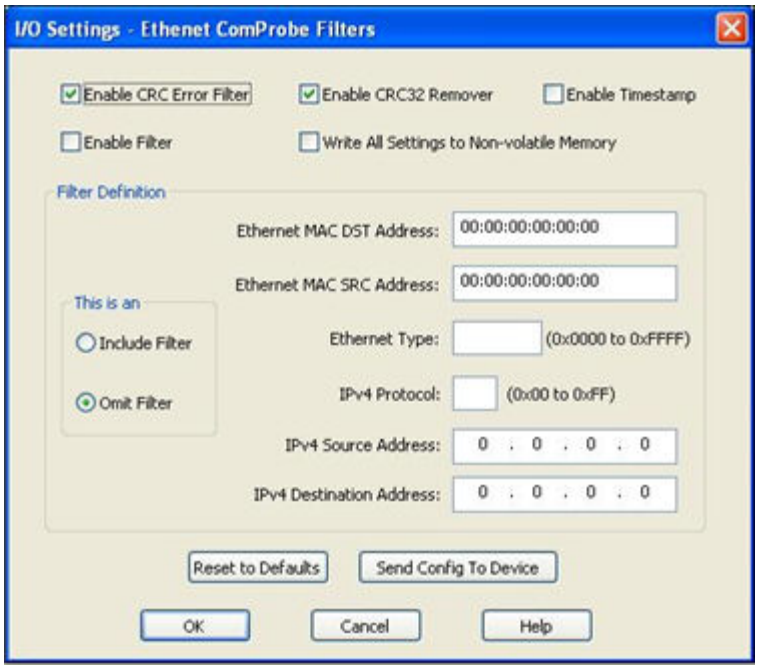
- You can select **Refresh List** at any time to update the list of devices.
- When you run NetDecoder with the **Ethernet ComProbe** option, the software disables the ability to sniff with other Ethernet NIC cards. If you wish to capture

Ethernet traffic over other NIC cards, you must select the regular **Ethernet** option in the NetDecoder start up wizard.

3.5.2 Ethernet ComProbe I/O Settings

The I/O Settings dialog allows you to configure the Ethernet ComProbe with filters and special timestamping ability.

1. You access the I/O Settings dialog by selecting I/O Settings from the Options menu on the NetDecoder Control window.



There are a number of settings you can select on this dialog that will affect how the frames are captured and displayed.

At the top of the dialog are five check boxes:

- **Enable CRC Error Filter:** When enabled, the CRC error filter discards all Ethernet frames that have CRC errors. These error frames will not be captured.
- **Enable CRC32 Remover:** When the CRC32 Remover is enabled, the Ethernet ComProbe removes the 4-bytes of CRC data from every Ethernet frame before passing it up to the software.
- **Enable Timestamp:** When enabled, the Ethernet ComProbe adds a five (5) NanoSecond timing to each capture packet. This also adds eight (8) extra bytes at the end of each Ethernet frame.
- **Enable Filter:** Selecting this check box either enables or disables the capture filters.

- **Write all settings to Permanent Memory:** If this option is selected, the configuration is written to the permanent non-volatile memory in the device.

This is an:

- **Include Filter**: When you select this radio button, the Ethernet packets that match the filter settings are captured and displayed.
- **Omit Filter**: When you select this radio button, the Ethernet packets that match the filter settings are discarded. Only packets that do not match the settings are captured and displayed.

On the right side are **six text entry boxes**:

- **Ethernet MAC DST Address:** Enter the Ethernet MAC Destination Address
- **Ethernet MAC SRC Address:** Enter the Ethernet MAC Source Address
- **Ethernet Type:** Enter the 2-byte Ethernet Type value in hex. The value can range from 0x0000 to 0xFFFF.
- **IPv4 Protocol:** Enter the one byte IPv4 protocol type. The value can range from 0x00 to 0xFF.

For a complete listing of the Ethernet Types and the IPv4 Protocol types, visit The Internet Assigned Numbers Authority (IANA) website (www.iana.org).

- **IPv4 Source Address:** Enter the Source IP Address
- **IPv4 Destination Address:** Enter the Destination IP Address

After selecting/entering values, it's very important that you understand what the buttons at the bottom of the dialog do when you select them.

- **Reset to Defaults**: When you select *Reset to Defaults*, Enable CRC Error Filter and Enable CRC32 Remover check boxes at the top of the dialog are enabled. All other options are disabled.
- **Send Config to Device**: After setting all the options in the dialog, you **must click on Send Config to Device before OK** to transfer the settings to the Ethernet ComProbe.
- **OK**: There are two things to consider with the **OK** button.
    - If you click OK **before** you select **Send Config to Device**, the dialog will close and the settings will be saved, but they **will not be transferred** to the ComProbe. The settings will, however, be there if you open the dialog again.
    - If you select OK **after** you select **Send Config to Device**, the dialog will close, the **settings will be saved and transferred to the ComProbe**.

- Selecting **Cancel** overrides all the selections and returns the user to the Control Window.

4 Protocol Stacks

4.1 Protocol Stack Wizard

The Protocol Stack wizard is where you define the protocol stack you want the analyzer to use when decoding frames.

To start the wizard:

1. Choose *Protocol Stack* from the *Options* menu on the Control window or click the Protocol Stack icon on the Frame Display.
2. Select a protocol stack from the list, and click Finish. Click for information on how the analyzer auto-traverses the protocol stack.

Most stacks are pre-defined here. If you have special requirements and need to set up a custom stack, see Creating a Custom Stack.

1. If you select a custom stack (i.e. one that was defined by a user and not included with the analyzer), the *Remove Selected Item From List* button becomes active.
2. Click the Remove button to remove the stack from the list. You cannot remove stacks provided with the analyzer. If you remove a custom stack, you need to define it again in order to get it back.

If you are changing the protocol stack for a capture file, you may need to reframe. See Reframing for more information.

You cannot select a stack or change an existing one for a capture file loaded into the Capture File Viewer (the Capture File Viewer is used only for viewing capture files and cannot capture data). Protocol Stack changes can only be made from a live session.

Note for BCSP:

If you are using the BCSP protocol stack, you must connect the analyzer to the circuit such that the data on the DTE line comes from the host, and data on the DCE line comes from the controller. Click here

Note for Modbus RTU:

If you are using the Modbus RTU protocol stack, you must select either Modbus RTU Master or Modbus RTU Slave depending on where the analyzer taps into the circuit. Click here for more information.

Note for Modbus TCP:

If you are using Modbus TCP over Ethernet, you need to set up a node database giving the IP addresses for the Master and Slave devices. Click here for more information.

Note for Data Highway Plus (DH+):

There are special hardware and software configuration instructions for setting up the DL3000 DHM device used to tap into the Data Highway Plus network. Click here for more information.

Note for IEC 870-5-101:

You need to give the decoder information on the sizes of some fields and whether or not other fields are present. There are all system configurable options and therefore the decoder has no way of knowing this information from the data. Click here for more information.

Note for DeviceNet

You need to install the DeviceNet card before beginning data capture. Then you need to setup the device in the Hardware Settings window, and optionally select any capture filters.

DeviceNet Card Installation Instructions

DeviceNet Device Setup

DeviceNet Capture Filters

4.2 Information Screen

The second screen of the Protocol Stack Wizard gives information to help you decide if you need to define a custom stack or if a pre-defined stack has what you need.

4.3 Creating and Removing a Custom Stack

To create a custom stack:

1. Choose *Protocol Stack* from the *Options* menu on the Control window or click the Protocol Stack icon on the Frame Display.
2. Select *Build Your Own* from the list and click *Next*.
3. The system displays an information screen that may help you decide if you need to define your own custom stack. Defining a custom stack means that the analyzer uses the stack for every frame. Frames that do not conform to the stack are decoded incorrectly. Click *Next* to continue.

Select Protocols

1. Select a protocol from the list on the left.
2. Click the right arrow button to move it to the Protocol Decode Stack box on the right, or double-click the protocol to move it to the right.
3. To remove a protocol from the stack, double-click it or select it and click the left arrow button.
4. If you need to change the order of the protocols in the stack, select the protocol you want to move, and click on the *Move Up* and *Move Down* buttons until the protocol is in the correct position.

5. The lowest layer protocol is at the top of the list, with higher layer protocols listed underneath.

Auto-traversal (Have the analyzer Determine Higher Layers)

If you need to define just a few layers of the protocol stack, and the remaining layers can be determined based on the lower layers:

1. Click the All additional stack layers can be determined automatically button.
2. If your protocol stack is complete and there are no additional layers, click the There are no additional stack layers button.
3. If you select this option, the analyzer uses the stack you defined for every frame. Frames that do use this stack are decoded incorrectly.

Save the Stack

To save your stack:

1. Click the Add To Predefined List button.
2. Give the stack a name, and click Add.

In the future, the stack appears in the Protocol Stack List on the first screen of the Protocol Stack wizard.

Remove a Stack

To remove the stack:

1. Select it in the first screen and click *Remove Selected Item From List*.
2. If you remove the stack, you must to recreate it if you need to use it again.

Note:

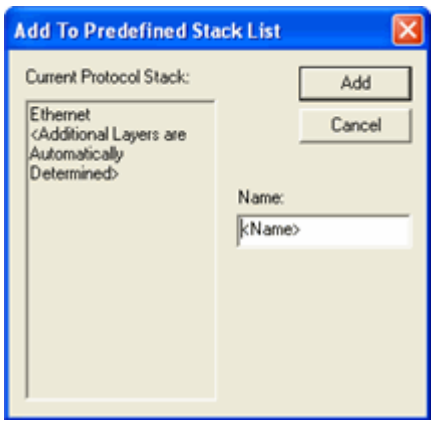
If you do not save your custom stack, it does appear in the predefined list, but applies to the frames in the current session. However, it is discarded at the end of the session.

4.4 Saving User Defined Stacks

You can create protocol stacks for one time use that disappear at the end of the session. If you want to use the stack again in a subsequent session, then you need to recreate it. However, if you save the stack, then it is available every time you start the analyzer, until you delete it.

The *Add To Predefined Stack List* dialog allows the user to save a custom stack for future use.

1. After creating a custom stack using the Protocol Stack Wizard, click the *Add To Predefined List* button on the last screen of the wizard.



Your newly defined stack appears in the *Current Protocol Stack* pane on the left.

2. Simply enter a name for the stack and click *Add*.

The name of the stack now appears as a selection in the *Select a Protocol Stack* dialog.

4.5 Reframing

If you need to change the protocol stack used to interpret a capture file and the framing is different in the new stack, you need to reframe in order for the protocol decode to be correct. You can also use Reframe to frame unframed data. The original capture file is not altered during this process.

Note: You cannot reframe from the Capture File Viewer (accessed by selecting Capture File Viewer or Load Capture File to start the software and used only for viewing capture files).

To reframe your data, load your capture file, select a protocol stack, and then select Reframe from the File menu on the Control window. Reframe is only available if the frame recognizer used to capture the data is different from the current frame recognizer.

In addition to choosing to Reframe, you can also be prompted to Reframe by the Protocol Stack Wizard.

1. Load your capture file by choosing Open from the File menu on the Control window, and select the file to load.
2. Select the protocol stack by choosing Protocol Stack from the Options menu on the Control window, select the desired stack and click Finish.
3. If you selected a protocol stack that includes a frame recognizer different from the one used to capture your data, the Protocol Stack Wizard asks you if you want to reframe your data. Choose Yes.
4. The analyzer adds frame markers to your data, puts the framed data into a new file, and opens the new file. The original capture file is not altered.

See Unframing for instructions on removing framing from data.

4.6 Unframing

This function removes start-of-frame and end-of-frame markers from your data. The original capture file is not altered during this process.

You cannot unframe from the Capture File Viewer (accessed by selecting Capture File Viewer or Load Capture File to start the software and used only for viewing capture files).

To manually unframe your data, select Unframe from the File menu on the Control window. Unframe is only available if a protocol stack was used to capture the data and there is currently no protocol stack selected.

In addition to choosing to Unframe, you can also be prompted to Unframe by the Protocol Stack Wizard.

1. Load your capture file. To do this, choose Open from the File menu on the Control window, and select the file to load.
2. Remove the protocol stack. To do this, choose Protocol Stack from the Options menu on the Control window, select None from the list, and click Finish.
3. The Protocol Stack Wizard asks you if you want to unframe your data and put it into a new file. Choose Yes.
4. The system removes the frame markers from your data, puts the unframed data into a new file, and opens the new file. The original capture file is not altered.

See Reframing for instructions on framing unframed data.

4.7 Providing Context For Decoding When Frame Information Is Missing

There may be times when you need to provide information to the analyzer because the context for decoding a frame is missing. For example, if the analyzer captured a response frame, but did not capture the command frame indicating the command.

The analyzer provides a way for you to supply the context for any frame, provided the decoder supports it. (The decoder writer has to include support for this feature in the decoder, so not all decoders support it. Note that not all decoders require this feature.)

If the decoder supports user-provided context, three items are active on the Options menu of the Control Window, Frame Display and Protocol Navigator windows. These items are *Set Initial Decoder Parameters*, *Automatically Request Missing Decoding Information*, and *Set Subsequent Decoder Parameters*. (These items are not present if no decoder is loaded that supports this feature.)

Set Initial Decoder Parameters is used to provide required information to decoders that is not context dependent but instead tends to be system options for the protocol.

Choose Set Initial Decoder Parameters in order to provide initial context to the analyzer for a decoder. A dialog appears that shows the data for which you can provide information.

If you need to change this information for a particular frame :

1. Right-click on the frame in the Frame Display window
2. Choose Provide <context name>.

Alternatively, you can choose Set Subsequent Decoder Parameter from the Options menu.

3. This brings up a dialog showing all the places where context data was overridden.
4. If you know that information is missing, you can't provide it, and you don't want to see dialogs asking for it, un-check *Automatically Request Missing Decoding Information*.
5. When unchecked, the analyzer doesn't bother you with dialogs asking for frame information that you don't have. In this situation, the analyzer decodes each frame until it cannot go further and then simply stop decoding.

5 Capturing Data

5.1 Capturing Data

Note: Data Capture is not available in Viewer mode.

1. Click the Start Capture icon to begin capturing to a file. This icon is located on the Control , Event Display , and Frame Display windows.
2. Files are placed in My Capture Files by default and have a .cfa extension. Choose Directories from the Options menu on the Control window to change the default file location.
3. Watch the status bar on the Control window to monitor how full the file is. When the file is full, it begins to *wrap*, which means the oldest data will be overwritten by new data.
4. Click the Stop icon to temporarily stop data capture. Click the Start Capture icon again to resume capture. Stopping capture means no data will be added to the capture file until capture is resumed, but the previously captured date remains in the file.
5. To clear captured data, click the Clear icon .
    - If you select Clear after selecting Stop, a dialog appears asking whether you want to save the data.
        - You can click Save File and enter a file name when prompted .
        - If you choose Do Not Save, all data will be cleared.
        - If you choose Cancel, the dialog closes with no changes.
    - If you select the Clear icon while a capture is occurring:
        - The capture stops.
        - A dialog appears asking if you want to save the capture
        - You can select Yes and save the capture or select No and close the dialog. In either case, the existing capture file is cleared and a new capture file is started.
        - If you choose Cancel, the dialog closes with no changes.

To change the size of the capture file, choose System Settings from the Options menu on the Control window.

6 Analyzing Byte Level Data

6.1 Event Display

To open this window

Click the Event Display icon on the Control window toolbar.

The Event Display window provides detailed information about every captured event. Events include data bytes, data related information such as start-of-frame and end-of-frame flags, and the analyzer information, such as when the Data Capture Was Paused. Data bytes are displayed in hex on the left side of the window, with the corresponding ASCII character on the right.

Click on an event to find out more about it. The three status lines at the bottom of the window are updated with information such as the time the event occurred (for data bytes, the time the byte was captured), the value of the byte in Hex, Decimal, Octal, and Binary, any errors associated with the byte, and more.

Events with errors are shown in red to make them easy to spot.

When capturing data live, the analyzer continually updates the Event Display as data is captured. Make sure the Lock icon is displayed on the toolbar to prevent the display from updating (Clicking on the icon again will unlock the display). While locked, you can review your data, run searches, determine delta time intervals between bytes, and check CRCs. To resume updating the display, click the Lock icon again.

You can have more than one Event Display open at a time. Click the Duplicate View icon to create a second, independent Event Display window. You can lock one copy of the Event Display and analyze your data, while the second Event Display updates as new data is captured.

6.2 The Event Display Toolbar

Home – Brings the Control window to the front.

Open File - Opens a capture file.

Start Capture - Begins data capture to disk.

Stop Capture - Closes a capture file and stops data capture to disk.

Save - Prompts user for a file name. If the user supplies a name, a .cfa file is saved.

Clear- Discards the temporary file and clears the display.

Lock - In the Lock state, the window is locked so you can review a portion of data. Data capture continues in the background. Clicking on the Lock icon unlocks the window.

Unlock - In the Unlock state, the screen fills in the data captured since the screen lock and moves down to display incoming data again. Clicking on the Unlock icon locks the window.

Duplicate View - Creates a second Event Display window identical to the first.

Frame Display - (framed data only) Brings up a Frame Display, with the frame of the currently selected bytes highlighted.

Focus Protocol Navigator - (framed data only) Brings up the Protocol Navigator window, with the currently selected frame highlighted.

Display Capture Notes - Brings up the Capture Notes window where you can view or add notes to the capture file.

Add/Modify Bookmark - Add a new or modify an existing bookmark.

Display All Bookmarks - Shows all bookmarks and lets you move between bookmarks.

Find - Search for errors, string patterns, special events and more.

Go To - Opens the Go To dialog, where you can specify which event number to go to.

CRC - Change the algorithm and seed value used to calculate CRCs. To calculate a CRC, select a byte range, and the CRC appears in the status lines at the bottom of the Event Display.

Mixed Sides - (Serial data only) By default, the analyzer shows data with the DTE side above the DCE side. This is called DTE over DCE format. DTE data has a white background and DCE data has a gray background. The analyzer can also

display data in mixed side format. In this format, the analyzer does not separate DTE data from DCE data but shows all data on the same line as it comes in. DTE data is still shown with a white background and DCE data with a gray background so that you can distinguish between the two. The benefit of using this format is that more data fits onto one screen.

Character Only - The analyzer shows both the number (hex, binary, etc.) data and the character (ASCII, EBCDIC or BAUDOT) data on the same screen. If you do not wish to see the hex characters, click on the Character Only button. Click again to go back to both number and character mode.

Number Only - Controls whether the analyzer displays data in both character and number format, or just number format. Click once to show only numeric values, and again to show both character and numeric values.

All Events - Controls whether the analyzer shows all events in the window, or only data bytes. Events include control signal changes and framing information.

Timestamping Options – Brings up the timestamping options window which has options for customizing the display and capture of timestamps.

6.3 Opening Multiple Event Display Windows

Click the Duplicate View icon from the Event Display toolbar to open a second Event Display window.

You can open as many Event Display windows as you like. Each Event Display is independent of the others and can show different data, use a different radix or character set, or be frozen or live.

The Event Display windows are numbered in the title bar. If you have multiple Event Displays open, click on the Event Display icon on the Control window toolbar to show a list of all the Event Displays currently open. Select a window from the list to bring it to the front.

6.4 Calculating CRCs or FCSs

The cyclic redundancy check (CRC) is a function on the Event Display window used to produce a checksum. The frame check sequence (FCS) are the extra checksum characters added to a frame to detect errors.

1. Open the Event Display window.
2. Click and drag to select the data you want to generate a CRC for.
3. Click on the CRC icon .

4. In the CRC dialog box, click on the down arrow to show the list of choices for CRC algorithms. Choose an algorithm to use. Choose CRC 32 (Ethernet). Choose CRC 32 (Ethernet) for Ethernet data or the appropriate CRC type for serial data.
5. Enter a seed value in hexadecimal if desired.
6. Click OK to generate the CRC. It appears in the byte information lines at the bottom of the Event Display window. Whenever you select a range of data, a CRC using the algorithm you selected is calculated automatically.

"CRC!" in Ethernet data

Ethernet network cards do not normally send the CRC with the frame to the upper layers of the system. The hardware on the card checks that the CRC is correct and then throws it away. FTS marks the place where the CRC would be in the data with "CRC!". When viewing Ethernet capture files made with other programs, the CRC may or may not be included, depending on the specifications of the capturing software/hardware.

Reversed CRCs on the Event Display with Ethernet data

The CRC calculated in the Event Display window is reversed from the CRC shown in the data. CRCs are calculated in network data order from Most Significant Byte (MSB) to Least Significant Byte (LSB). The Ethernet specification says to send data in host data order (LSB to MSB). Therefore the CRC as captured in the data is the reverse of the CRC as calculated.

Example: If the CRC in the data is shown as 00 01 02 03, the Event Display calculated the CRC and show it in the status lines as 03 02 01 00. This is correct.

Calculating CRC for interwoven data

FTS calculates the CRC for either side of the interwoven data. Which side it calculates is determined by the first byte selected. If the first byte is from one side, then FTS calculates the CRC for just the bytes on that side. If the first byte is from the other side, then FTS calculates the CRC for just the bytes on that side.

Incorrect results with CRC16 for serial data

If you are calculating CRCs using the CRC16 algorithm and the CRCs do not match what you know they should be, try CRC16rev. What hardware often calls CRC16 is what software calls CRC16rev.

6.5 Calculating Delta Times and Data Rates

1. Click on the Event Display icon on the Control window to open the Event Display window.
2. Use the mouse to select the data you want to calculate a delta time and rate for.
3. The Event Display window displays the delta time and the data rate in the status lines at the bottom of the window.

6.6 Switching Between Live Update and Review Mode

The Event Display and Frame Display windows can update to display new data during live capture, or be frozen to allow data analysis. By default, the Event Display continually updates with new data, and the Frame Display is locked.

1. Make sure the Lock icon is active so the display is locked and unable to scroll.
2. Click the Unlock icon again to resume live update.

The analyzer continues to capture data in the background while the display is locked. Upon resuming live update, the display updates with the latest data.

You can have more than one Event Display or Frame Display window open at a time. Click the Duplicate View icon to open additional Event or Frame Display windows. The Lock/Resume function is independent on each window. This means that you can have two Event Display windows open simultaneously, and one window can be locked while the other continues to update.

6.7 Data Formats and Symbols

6.7.1 Switching Between Viewing All Events and Viewing Data Events

By default, the analyzer on the Event Display dialog shows all *events*.

This includes:

- Data bytes
- Start-of-frame
- End-of-frame characters
- Data Captured Was Paused.

Click on the Display All Events icon to remove the non-data events. Click again to display all events.

See List of All Event Symbols for a list of all the special events shown in the analyzer and what they mean.

6.7.2 Switching Between Hex, Decimal, Octal or Binary

On the Event Display window the analyzer displays data in Hex by default. There are several ways to change the *radix* used to display data.

1. Go to the View menu and select the radix you want. A check mark next to the radix indicates which set is currently being used.
2. Right-click on the "Hex" header label and choose a different radix.

If you want to see only the numerical values, click on the Numbers Only icon on the Event Display toolbar.

6.7.3 Switching Between ASCII, EBCDIC, and Baudot

On the Event Display window, the analyzer displays data in ASCII by default. There are several ways to change the character set used to display data.

1. Go to the View menu and select the character set you want. A check mark next to the character set indicates which set is currently being used.
2. Right-click on the "ASCII" header label and choose a different character set.

If you want to see only characters, click on the Characters Only icon on the Event Display toolbar.

6.7.4 Viewing Only ASCII (or EBCDIC or Baudot)

On the Event Display toolbar you can choose to view data in ASCII, EBCDIC, or Baudot format only.

1. Click on the Characters Only icon on the Event Display toolbar.

To add the numerical values back to the display:

1. Click the Characters Only icon again.

6.7.5 Viewing Only Hex (Or Decimal or Octal or Binary)

On the Event Display toolbar you can choose to view data as numeric only.

1. Click on the Numbers Only icon on the Event Display toolbar.

To display the characters back to the display:

1. Click the Number Only icon again.

6.7.6 Selecting Mixed Channel/Sides

If you want to get more data on the Event Display window, you can switch to mixed sides mode. This mode puts all the data together on the same line. Data from one side is shown on a white background and data from the other is shown on a gray background.

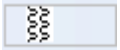
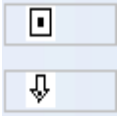
1. Click once on the Mixed Sides icon to put the display in mixed sides mode.
2. Click again to return to side over side mode.
3. You can right click on the labels in the center of the data display window to change between mixed and side over side modes.
4. Choose Display Sides Together to go to Mixed Sides Mode or Display Sides Separately to go to side over side mode.

6.7.7 List of All Event Symbols

By default, the Event Display shows all *events*, which includes control signal changes, start and end of frame characters and flow control changes. If you want to see only the data bytes, click on the All Events button . Click again to display all events.

Click on a symbol, and the analyzer displays the symbol name and sometimes additional information in the status lines at the bottom of the Event Display window. For example, clicking on a control signal change symbol displays which signal(s) changed.

In addition to data bytes, the events shown are (in alphabetical order):

	Abort
	Broken Frame - The frame did not end when the analyzer expected it to. This occurs most often with protocols where the framing is indicated by a specific character, control signal change, or other data related event.
	Buffer Overflow - Indicates a buffer overflow error. A buffer overflow always causes a broken frame.
	Control Signal Change - One or more control signals changed state. Click on the symbol, and the analyzer displays which signal(s) changed at the bottom of the Event Display window.
	Data Capture Paused - The Pause icon was clicked, pausing data capture. No data is recorded while capture is paused.
	Data Capture Resumed - The Pause icon was clicked again, resuming data capture.
	Dropped Frames - Some number of frames were lost. Click on the symbol, and the analyzer displays many frames were lost at the bottom of the Event Display window.
	End of Frame - Marks the end of a frame.
	Flow Control Active - An event occurred which caused flow control to become active (i.e. caused the analyzer to stop transmitting data) Events which activate flow control are signal changes or the receipt of an XON character.
	Flow Control Inactive - An event occurred which caused flow control to become inactive (i.e. caused the analyzer to transmit data). Events which deactivate flow control are signal changes or the receipt of an XOFF character.
	Frame Recognizer Change - A lowest layer protocol was selected or removed here, causing the frame recognizer to be turned off or on.

6.7.8 Font Size

The font size can be changed on several windows. Changing the font size on one window does not affect the font size on any other window.

To change the font size:

1. Click on *Options,* and select Change the Font Size.
2. Choose a font size from the list.
3. Click OK.

7 Analyzing Protocol Decodes

7.1 Frame Display Window

7.1.1 Frame Display Window

To open this window

Click the Frame Display icon on the Control window toolbar, or select Frame Display from the Window menu.

Frame Display Panes

The Frame Display window is used to view all frame related information. It is composed of a number of different sections or "panes", where each pane shows a different type of information about a frame. The image below gives the name of each pane. Click on the links below the image to learn more about each pane.

- Summary Pane

  The Summary Pane displays a one line summary of each frame for every protocol found in the data, and can be sorted by field for every protocol. Click here for an explanation of the symbols next to the frame numbers.

- Decode Pane

  The Detail Pane displays a detailed decode of the highlighted frame. Fields selected in the Decode pane have the appropriate bit(s) or byte(s) selected in the Radix, Binary, Character and Event panes.

- Radix Pane

  The Radix Pane displays the logical data bytes in the selected frame in either hexadecimal, decimal or octal.

- Binary Pane

  The Binary Pane displays a binary representation of the logical data bytes.

- Character Pane

  The Character Pane displays the character representation of the logical data bytes in either ASCII, EBCDIC or Baudot.

- Event Pane

  The Event Pane displays the physical data bytes in the frame, as received on the network.

By default, all panes except the Event pane are displayed when the Frame Display is first opened.

Protocol Tabs

The Frame Display adds a tab to the top of the Summary Pane for every protocol found in the in the data. You can click on these tabs to filter on the protocol. Select the Unfiltered tab to display all protocols. The Unfiltered tab is automatically selected when multiple protocols are being *filtered-in* using other filtering methods.

Comparing Frames

If you need to compare frames, you can open additional Frame Display windows by clicking on the Duplicate View icon . You can have as many Frame Display windows open at a time as you wish.

7.1.2 Frame Display Toolbar

The buttons that appear in the Frame Display window vary according to the particular configuration of the analyzer.

Home – Brings the Control window to the front.

Open File - Opens a capture file.

I/O Settings - Opens the I/O Settings dialog.

Start Capture - Begins data capture to a user designated file.

Stop Capture - Closes a capture file and stops data capture to disk.

Save - Save the currently selected bytes or the entire buffer to file.

Clear- Discards the temporary file and clears the display.

Event Display – Brings the Event Display window to the front.

Protocol Navigator – Brings the Protocol Navigator window to the front.

Statistics - Brings the Statistics window to the front. This icon does not display in this location when running the analyzer in Air Sniffer. See Packet Error Rate Statistics below.

Signal Display - Opens the Signal Display. This icon does not display when running the analyzer in Air Sniffer.

Breakout Box - Opens the Breakout Box dialog.

Duplicate View - Creates a second Frame Display window identical to the first.

Apply/Modify Display Filters - Opens the Display Filter dialog.

Quick Protocol Filter - brings up a dialog box where you can filter or hide one or more protocol layers.

Find - Search for errors, string patterns, special events and more.

Display Capture Notes - Brings up the Capture Notes window where you can view or add notes to the capture file.

Add/Modify Bookmark - Add a new or modify an existing bookmark.

Display All Bookmarks - Shows all bookmarks and lets you move between bookmarks.

Protocol Stack - brings up the Protocol Stack Wizard where you can change the stack used to decode framed data

Reload Decoders - When Reload Decoders is clicked, the plug-ins are reset and received frames are redecoded. For example, If the first frame occurs more than 10 minutes in the past, the 10-minute utilization graph stays blank until a frame from 10 minutes ago or less is decoded.

Packet Timeline – Opens the Packet Timeline display.

Extract Data - Opens the Extract Data dialog.

Packet Error Rate Statistics - Opens the Packet Error Rate Statistics display.

Audio Extraction - Opens the Audio Extraction dialog.

Pie Chart - This icon displays a chart that displays the number of frames with and without errors.

Network View - Opens the Network View Window.

Dashboard - Opens the Dashboard Dialog

Filter: Text giving the filter currently in use. If no filter is being used, the text reads "All Frames" which means that nothing is filtered out. To see the text of the entire filter, place the cursor over the text and a ToolTip pops up with the full text of the filter.

The following icons all change how the panes are arranged on the Frame Display. Additional layouts are listed in the View menu.

Show Default Panes - Returns the panes to their default settings.

Show Only Summary Pane - Displays only the Summary pane.

Toggle Expanded Decode Pane - Makes the Decode pane taller and the Summary pane narrower.

Toggle Display Freeze - Prevents the display from updating.

Go To Frame - Opens the Go To dialog, where you can specify which event number to go to.

First Frame - Moves to the first frame in the buffer.

Previous Frame - Moves to the previous frame in the buffer.

Next Frame - Moves to the next frame in the buffer.

Last Frame - Moves to the last frame in the buffer.

Note that if the frames are sorted in other than ascending frame number order, the order of the frames in the buffer is the sorted order. Therefore the last frame in the buffer may not have the last frame number.

Summary drop-down box

Lists all the protocols found in the data in the file. This box does not list all the protocol decoders available to the analyzer, merely the protocols found in the data. Selecting a protocol from the list changes the Summary pane to display summary information for that protocol. When a FBLEA predefined Named Filter (like Nulls and Polls) is selected, the Summary drop-down is disabled.

Text with Protocol Stack

To the right of the Summary Layer box is some text giving the protocol stack currently in use.

7.1.3 Frame Display Status Bar

The Frame Display Status bar appears at the bottom of the Frame Display. It contains the following information:

- Total Frames: The total number of frames in the capture buffer or capture file in real-time
- Frames Filtered In: The total number of frames displayed in the filtered results from user applied filters in real-time
- Frame #s Selected: Displays the frame number or numbers of selected (highlighted) frames, and the total number of selected frames in parentheses

7.1.4 Hiding and Revealing Protocol Layers in the Frame Display

Hiding protocol layers refers to the ability to prevent a layer from being displayed on the Decode pane. Hidden layers remain hidden for every frame where the layer is present, and can be revealed again at any time. You can hide as many layers as you wish.

Note: Hiding from the Frame Display affects only the data shown in the Frame Display and not any information in any other window.

There are two ways to hide a layer.

1. Right-click on the layer in the Decode pane, and choose Hide [protocol name] Layer In All Frames.
2. Click the Set Protocol Filtering button on the Summary pane toolbar. In the Protocols to Hide box on the right, check the protocol layer(s) you want hidden. Click OK when finished.

To reveal a hidden protocol layer:

1. Right-click anywhere in the Decode pane
2. Choose Show [protocol name] Layer from the right-click menu, or click the Set Protocol Filtering button and un-check the layer or layers you want revealed.

7.1.5 Physical vs. Logical Byte Display

The Event Display window and Event Pane in the Frame Display window show the *physical bytes*. In other words, they show the actual data as it appeared on the circuit. The Radix, Binary and Character panes in the Frame Display window show the *logical data*, or the resulting byte values after escape codes or other character altering codes have been applied (a process called *frame transformation*).

As an example, bytes with a value of less than 0x20 (the 0x indicates a hexadecimal value) cannot be transmitted in Async PPP. To get around this, a 0x7d is transmitted before the byte. The 0x7d says to take the next byte and subtract 0x20 to obtain the true value. In this situation, the Event pane displays 0x7d 0x23, while the Radix pane displays 0x03.

7.1.6 Sorting Frames

By default, frames are sorted in ascending numerical sequence by frame number. Click on a column header in the Summary pane to sort the frames by that column. For example, to sort the frames by size, click on the *Frame Size* column header.

An embossed triangle next to the header name indicates which column the frames are sorted by. The direction of the triangle indicates whether the frames are in ascending or descending order, with up being ascending.

Note that it may take some time to sort large numbers of frames.

7.1.7 Synchronizing the Event and Frame Displays

The Frame Display is synchronized with the Event Display. Click on a frame in the Frame Display and the corresponding bytes is highlighted in the Event Display. Each Frame Display has its own Event Display.

As an example, here's what happens if the following sequence of events occurs.

1. Click on the Frame Display icon in Control window toolbar to open the Frame Display.
2. Click on the Duplicate View icon to create Frame Display #2.
3. Click on Event Display icon in Frame Display #2. Event Display #2 opens. This Event Display is labeled #2, even though there is no original Event Display, to indicate that it is synchronized with Frame Display #2.
4. Click on a frame in Frame Display #2. The corresponding bytes are highlighted in Event Display #2.
5. Click on a frame in the original Frame Display. Event Display #2 does not change.

7.1.8 Working With Multiple Frame Displays

Multiple Frame Displays are useful for comparing two frames side by side. They are also useful for comparing all frames against a filtered subset or two filtered subsets against each other.

- To create a second Frame Display, click the *Duplicate View* icon on the Frame Display toolbar.

This creates another Frame Display window. You can have as many Frame Displays open as you wish. Each Frame Display is given a number in the title bar to distinguish it from the others.

- To navigate between multiple Frame Displays, click on the *Frame Display* icon in the Control window toolbar.

A drop-down list appears, listing all the currently open Frame Displays.

- Select the one you want from the list and it comes to the front.

Note: When you create a filter in one Frame Display, that filter does not automatically appear in other Frame Display windows. You must use the Hide/Reveal feature to display a filter created in one Frame Display in different Frame Display window.

7.1.9 Working With Panes

When the Frame Display first opens, all panes are displayed except the Event pane. The panes include:

- To view all the panes, select *Show All Panes* from the *View* menu.
- The *Toggle Expand Decode Pane* icon makes the decode pane longer to view lengthy decodes better.
- The *Show Default Panes* icon returns the Frame Display to its default settings.
- The *Show only Summary Pane* icon displays on the Summary Pane.

1. To close a pane, right-click on the pane and select *Hide This Pane* from the pop-up menu, or de-select *Show [Pane Name]* from the *View* menu.
2. To open a pane, right-click on the any pane and highlight *Show Hidden Panes* from the pop-up menu and select the pane from the fly-out menu, or select *Show [Pane Name]* from the *View* menu.
3. To resize a pane, place the cursor over the pane border until a double-arrow cursor appears. Click and drag on the pane border to resize the pane.

7.1.10 The Panes in the Frame Display

7.1.10.1 Summary Pane

The Summary pane displays a one-line summary of every frame in a capture buffer or file, including frame number, timestamp, length and basic protocol information. The protocol information included for each frame depends on the protocol selected in the summary layer box (located directly below the main toolbar).

On a two-channel circuit, the background color of the one-line summary indicates whether the frame came from the DTE or the DCE device. Frames with a white background come from the DTE device, frames with a gray background come from the DCE device.

The Summary pane in FTS4USB displays a one-line summary of every transaction in a capture buffer or file. Whenever there is a transaction it is shown on a single line instead of showing the separate messages that comprise the transaction. The Msg column in that case says "Transaction".

Each message in a transaction contains a packet identifier (PID). All of the PIDs in a transaction are shown in the transaction line.

All IN transactions (i.e. transactions that contain an IN token message) are shown with a purple background. All other transactions and all non-transactions are shown with a white background. IN transactions have special coloring because that is the only place where the primary data flow is from a device to the Host.

The protocol information included for each frame depends on the protocol selected in the summary layer box (located directly below the main toolbar).

Frame numbers in red indicate errors, either physical (byte-level) or frame errors. If the error is a frame error in the displayed protocol layer, the bytes where the error occurred is displayed in red. The Decode Pane gives precise information as to the type of error and where it occurred.

The Summary pane is synchronized with the other panes in this window. Click on a frame in the Summary pane, and the bytes for that frame is highlighted in the Event pane while the Decode pane displays the full decode for that frame. Any other panes which are being viewed are updated accordingly. If you use one pane to select a subset of the frame, then only that subset of the frame is highlighted in the other panes.

Use the navigation icons, keyboard or mouse to move through the frames. The icons and move you to the first and last frames in the buffer, respectively. Use the Go To icon to move to a specific frame number.

7.1.10.2 Customizing Fields in the Summary Pane

You can modify the Summary Pane in Frame Display.

Changing Column Widths

To change the width of a column:

1. Place the cursor over the right column divider until the cursor changes to a solid double arrow.
2. Click and drag the divider to the desired width.
3. To auto-size the columns, double-click on the column dividers.

Hiding Columns

To hide a column:

1. Drag the right divider of the column all the way to the left.
2. The cursor changes to a split double arrow when a hidden column is present.
3. To show the hidden column, place the cursor over the divider until it changes to a split double arrow, then click and drag the cursor to the right.
4. The Frame Size, Timestamp, and Delta columns can be hidden by right-clicking on the header and selecting *Show Frame Size Column, Show Timestamp Column,* or *Show Delta Column*. Follow the same procedure to display the columns again.

Moving Columns - Changing Column Order

To move a column :

1. Click and hold on the column header
2. Drag the mouse over the header row.
3. A small white triangle indicates where the column is moved to.
4. When the triangle is in the desired location, release the mouse.

Restoring Default Column Settings

To restore columns to their default locations, their default widths, and show any hidden columns

1. Right-click on any column header and choose *Restore Default Column Widths*, or select *Restore Default Column Widths* from the *Format* menu.

7.1.10.3 Frame Symbols in the Summary Pane

A green dot means the frame was decoded successfully, and the protocol listed in the Summary Layer drop-down box exists in the frame. No dot means the frame was decoded successfully, but the protocol listed in the Summary Layer drop-down box does not exist in the frame.

A green circle means the frame was not fully decoded. There are several reasons why this might happen.

One reason is that the frame compiler hasn't caught up to that frame yet. It takes some time for the analyzer to compile and decode frames. Frame compilation also has a lower priority than other tasks, such as capturing data. If the analyzer is busy capturing data, frame compilation may fall behind. When the analyzer catches up, the green circle changes to either a green dot or no dot.

Another reason is if some data in the frame is context dependent and we don't have the context. An example is a compressed header where the first frame gives the complete header, and subsequent frames just give information on what has changed. If the analyzer does not capture the first frame with the complete

header, it cannot decode subsequent frames with partial header information.

A magenta triangle indicates that a bookmark is associated with this frame. Any comments associated with the bookmark appear in the column next to the bookmark symbol.

7.1.10.4 Frame Display - Right Click Filtering

In Frame Display, protocols are displayed as tabs in the Summary Pane. When you select a tab, the protocol layers are displayed. The layers vary depending on the protocol.

You can create additional protocol tabs that highlight specific layers in the Summary Pane using the **Filtering Results** dialog.

Note: The Filtering Results dialog is not available for all layers because the information within those layers is not sortable, like time.

To use the Filtering Results dialog:

1. Right-click on a value in the Summary Pane. For example, the "S" for Slave under Role
2. On the drop-down list select **Filter in "Name = Value"**

Note: The "Name" and "Value" change depending on the layer.

The Filtering Results dialog appears.

3. Enter a name for the Filter.
4. Select OK.

A new protocol tab with the Filter Name you just created appears in the Summary Pane. The new tab displays data specific to the layer you selected.

7.1.10.5 Decode Pane

The Decode pane (aka detail pane) is a post-process display that provides a detailed decode of each frame transaction (sometimes referred to as a frame). The decode is presented in a layered format that can be expanded and collapsed depending on which layer or layers you are most interested in. Click on the plus sign to expand a layer. The plus sign changes to a minus sign. Click on the minus sign to collapse a layer. Select Show All or Show Layers from the Format menu to expand or collapse all the layers. Layers retain their expanded or collapsed state between frames.

Protocol layers can be hidden, preventing them from being displayed on the Decode pane. Right-click on any protocol layer and choose Hide [protocol name] from the right-click menu.

In a USB transaction, all messages that comprise the transaction are shown together in the detail pane. The color coding that is applied to layers when the detail pane displays a single message is applied to both layers and messages when the detail pane displays a transaction. To keep the distinction between layers and messages clear, each header of each message in the detail pane ends with the word “Message” or “Messages”. The latter is used because data and handshake messages are shown as a single color-coded entry

Each protocol layer is represented by a color, which is used to highlight the bytes that belong to that protocol layer in the Event, Radix, Binary and Character Panes. The colors are not assigned to a protocol, but are assigned to the layer.

The Event, Radix, Binary, Character and Decode panes are all synchronized with one another. Clicking on an element in any one of the panes highlights the corresponding element in all the other panes.

Click the Toggle Expand Decode Pane icon to make the Decode pane taller. This allows for more of a lengthy decode to be viewed without needing to scroll.

Searching for Patterns in the Decode

Hiding and Revealing Protocol Layers

What the Color of the Data Bytes means

Changing Protocol Layer Colors

Working With Panes (changing pane layouts, resizing panes)

7.1.10.6 Radix or Hexadecimal Pane

The Radix pane displays the logical bytes in the frame in either hexadecimal, decimal or octal. The radix can be changed from the Format menu, or by right-clicking on the pane and choosing Hexadecimal, Decimal or Octal.

Because the Radix pane displays the logical bytes rather than the physical bytes, the data in the Radix pane may be different from that in the Event pane. See Physical vs. Logical Byte Display for more information.

Colors are used to show which protocol layer each byte belongs to. The colors correspond to the layers listed in the Decode pane.

The Event, Radix, Binary, Character and Decode panes are all synchronized with one another. Clicking on an element in any one of the panes highlights the corresponding element in all the other panes.

What the Color of the Data Bytes mean

Changing Protocol Layer Colors

Working With Panes (changing pane layouts, resizing panes)

7.1.10.7 Character Pane

The Character pane represents the logical bytes in the frame in ASCII, EBCDIC or Baudot. The character set can be changed from the Format menu, or by right-clicking on the pane and choosing the appropriate character set.

Because the Character pane displays the logical bytes rather than the physical bytes, the data in the Character pane may be different from that in the Event pane. See Physical vs. Logical Byte Display for more information.

Colors are used to show which protocol layer each byte belongs to. The colors correspond to the layers listed in the Decode pane.

The Event, Radix, Binary, Character and Decode panes are all synchronized with one another. Clicking on an element in any one of the panes highlights the corresponding element in all the other panes.

7.1.10.8 Binary Pane

The Binary pane displays the logical bytes in the frame in binary. This pane is synchronized with the Decode pane so that individual bit fields can be highlighted.

Because the Binary pane displays the logical bytes rather than the physical bytes, the data in the Binary pane may be different from that in the Event pane. See Physical vs. Logical Byte Display for more information.

Colors are used to show which protocol layer each byte belongs to. The colors correspond to the layers listed in the Decode pane.

The Event, Radix, Binary, Character and Decode panes are all synchronized with one another. Clicking on an element in any one of the panes highlights the corresponding element in all the other panes.

7.1.10.9 Event Pane

The Event pane shows the physical bytes in the frame. You can choose between displaying only the data events or displaying all events by clicking the All Events icon .

Displaying all events means that special events, such as Start of Frame/End of Frame and any signal change events, are displayed as special symbols within the data.

The status lines at the bottom of the pane give the same information as the status lines in the Event Display window. This includes physical data errors, control signal changes (if appropriate), and timestamps.

Because the Event pane displays the physical bytes rather than the logical bytes, the data in the Event pane may be different from that in the Radix, Binary and Character panes. See Physical vs. Logical Byte Display for more information.

Colors are used to show which protocol layer each byte belongs to. The colors correspond to the layers listed in the Decode pane.

The Event, Radix, Binary, Character and Decode panes are all synchronized with one another. Clicking on an element in any one of the panes highlights the corresponding element in all the other panes.

7.1.11 Protocol Layer Colors

7.1.11.1 Data Byte Color Notation

The color of the data in the panes specifies which layer of the protocol stack the data is from. All data from the first layer is bright blue, the data from the second layer is green, the third layer is pink, etc. The protocol name for each layer in the Decode pane is in the same color. Note that the colors refer to the layer, not to a specific protocol. In some situations, a protocol may be in two different colors in two different frames, depending on where it is in the stack. You can change the default colors for each layer.

Red is reserved for bytes or frames with errors. In the Summary pane, frame numbers in red mean there is an error in the frame. This could be a physical error in a data byte or an error in the protocol decode. Bytes in red in the Radix, Character, Binary and Event panes mean there is a physical error associated with the byte.

7.1.11.2 Red Frame Numbers and Bytes

Red is reserved for bytes or frames with errors. In the Summary pane, frame numbers in red mean there is an error in the frame. This could be a physical error in a data byte or an error in the protocol decode. Bytes in red in the Radix, Character, Binary and Event panes mean there is a physical error associated with the byte.

7.1.11.3 Changing Protocol Layer Colors

You can differentiate different protocol layers in the Decode, Event, Radix, Binary and Character panes.

1. Choose *Select Colors* from the Options menu to change the colors used
2. To change a color, click on the arrow next to each layer and select a new color.

7.1.12 Protocol Filtering from the Frame Display

7.1.12.1 Easy Protocol Filtering

There are two types of easy protocol filtering. The first method lets you filter on the protocol shown in the *Summary* pane, and the second lets you filter on any protocol discovered on the network so far.

Filtering On the Summary Layer Protocol

Quick Filtering on a Protocol Layer / Filtering on all Frames with Errors

7.1.12.2 Filtering On the Summary Layer Protocol

To filter on the protocol in the *Summary* in the Frame Display window pane:

1. Select the tab of the desired protocol, or open the *Summary Layer* combo box.
2. Select the desired protocol.
3. To filter on a different layer, just select another tab, or change the layer selection in the combo box.

7.1.12.3 Quick Filtering on a Protocol Layer

1. To filter on any protocol layer, open either the *Frame Display* or *Protocol Navigator* window.
2. On the *Frame Display* window, click the starred *Quick Filtering* icon or select "Quick Filtering" from the *Filter* menu.

This opens a dialog that lists all the protocols discovered so far. The protocols displayed change depending on the data received.

The box on the left is **Protocols To Filter In**.

- When you select the checkbox for a protocol in the **Protocols to Filter In**, the Summary Pane will only display those frames that contain data from that protocol.

If you filter on more than one protocol, the result are all frames that contain at least one of those protocols. For example, if you filter on IP and IPX NetBIOS, you receive all frames that contain either IP or IPX NetBIOS (or both). A Quick Filter tab then appears on the Frame Display labeled Quick Filter. Changing the filter definition on the Quick Filter dialog changes the filter applied on the Quick Filter tab. Quick filters are persistent during the session, but are discarded when the session is closed.

The box in the center is the **Protocols To Hide**.

- When you select the checkbox for a protocol in the **Protocols To Hide**, data for that protocol will not appear in the Decode, Binary, Radix, and Character Panes. The frames containing that type data will still appear in the Summary Pane, but not in the Decode, Binary, Radix, and Character Panes.

The box on the right is the **Named Filters**. It contains filters that you create using the Named Filter and Set Condition dialogs.

- When you select the checkbox for the Name Filters, a tab appears on the Summary Pane that displays the frame containing the specific data identified in the filter. The named Filter tab remains on the Frame Display Summary Pane unless you hide it using the Hide/Show Display Filters dialog.

With **FBLEA**, the Configured BT Low energy devices and Exclude NULLSs and POLLs are default named filters.

1. Check the small box next to the name of each protocol you want to filter in, hide, or Named Filter to display.
2. Then click *OK*.

7.1.12.4 Filtering on all Frames with Errors from the Frame Display

To filter on all frames with errors:

1. Open the *Frame Display* window.
2. Click the starred *Quick Filter* icon or select "Quick Filtering" from the *Filter* menu
3. Check the box for *All Frames With Errors* in the "Protocols to filter in" pane, and click *OK.*
4. The system creates a tab on the *Frame Display* labeled *Quick Filter* that displays the results of the *All Frames With Errors* filter.

7.1.12.5 Frame Display - Right Click Filtering

In Frame Display, protocols are displayed as tabs in the Summary Pane. When you select a tab, the protocol layers are displayed. The layers vary depending on the protocol.

You can create additional protocol tabs that highlight specific layers in the Summary Pane using the **Filtering Results** dialog.

Note: The Filtering Results dialog is not available for all layers because the information within those layers is not sortable, like time.

To use the Filtering Results dialog:

1. Right-click on a value in the Summary Pane. For example, the "S" for Slave under Role
2. On the drop-down list select **Filter in "Name = Value"**

Note: The "Name" and "Value" change depending on the layer.

The Filtering Results dialog appears.

3. Enter a name for the Filter.
4. Select OK.

A new protocol tab with the Filter Name you just created appears in the Summary Pane. The new tab displays data specific to the layer you selected.

7.2 Protocol Navigator Window

7.2.1 Protocol Navigator

The *Protocol Navigator* displays the decode for more than one frame at a time, and has several features for controlling which frames and/or parts of frames are displayed. The main part of the window displays the decode for multiple frames. When you first open the window, every protocol layer of every frame is collapsed. By expanding the protocols, the *Protocol Navigator* displays the equivalent of the *Decode* pane on the *Frame Display*, with the added convenience of displaying multiple frame decodes in one place.

Click the *Protocol Navigator* icon to display the *Protocol Navigator*.

There are three methods for controlling the display in the *Protocol Navigator;* expanding/collapsing protocols, filtering, and hiding.

7.2.2 Protocol Navigator Toolbar

The buttons that appear in the Protocol Navigator window vary according to the particular configuration of the analyzer.

Home – Brings the Control window to the front.

Open File - Opens a capture file.

I/O Settings - Opens the I/O Settings dialog.

Start Capture - Begins data capture to a user designated file.

Stop Capture - Closes a capture file and stops data capture to disk.

Save - Save the currently selected bytes or the entire buffer to file.

Clear- Discards the temporary file and clears the display.

Event Display – Brings the Event Display window to the front.

Frame Display - (framed data only) Opens a Frame Display, with the frame of the currently selected bytes highlighted.

Breakout Box - Opens the Breakout Box dialog.

Duplicate View - Creates a second Frame Display window identical to the first.

Apply/Modify Display Filters - Opens the Display Filter dialog.

Quick Protocol Filter - brings up a dialog box where you can filter or hide one or more protocol layers.

Find - Search for errors, string patterns, special events and more.

Display Capture Notes - Brings up the Capture Notes window where you can view or add notes to the capture file.

Add/Modify Bookmark - Add a new or modify an existing bookmark.

Display All Bookmarks - Shows all bookmarks and lets you move between bookmarks.

Protocol Stack - brings up the Protocol Stack Wizard where you can change the stack used to decode framed data

Reload Decoders - When Reload Decoders is clicked, the plug-ins are reset and received frames are redecoded. For example, If the first frame occurs more than 10 minutes in the past, the 10-minute utilization graph stays blank until a frame from 10 minutes ago or less is decoded.

Packet Timeline – Opens the Packet Timeline display.

Extract Data - Opens the Extract Data dialog.

Packet Error Rate Statistics - Opens the Packet Error Rate Statistics display.

Audio Extraction - Opens the Audio Extraction dialog.

Network View - Opens the Network View Window.

Dashboard - Opens the Dashboard Dialog

The following icons all change how the panes are arranged on Protocol Navigator. Additional layouts are listed in the View menu.

First Frame - Moves to the first frame in the buffer.

Previous Frame - Moves to the previous frame in the buffer.

Next Frame - Moves to the next frame in the buffer.

Last Frame - Moves to the last frame in the buffer.

Protocol Navigator

Protocol Navigator Status Bar

7.2.3 Protocol Navigator Status Bar

The Protocol Navigator Status bar appears at the bottom of the Protocol Navigator. It contains the following information:

- Total Frames: The total number of frames in the capture buffer or capture file in real-time
- Frames Filtered In: The total number of frames displayed in the filtered results from user applied filters in real-time
- Frame #s Selected: Displays the frame number(s) of selected (highlighted) frames, and the total number of selected frames in parentheses.

7.2.4 The Difference Between Filtering and Hiding

You can filter on one or more protocol layers. The filter is inclusive, which means that filtering on a protocol means that only frames that contain that protocol are shown in the window. Frames that do not contain the protocol do not appear. You can filter on one protocol or several. (Filtering on the Protocol Navigator window is display filtering only.)

Hiding means that the selected layer is not displayed in the window, even though it may be present in the frame. This allows you to zoom in on a particular layer by hiding every layer but the one of interest.

An example using the IP stack may help to illustrate the difference. Assume that you only want to see frames that have TCP in them. You create a filter on TCP. The results displayed in the Protocol Navigator (or Frame Display) window have only those frames that carry TCP.

Now you're ready to look at the TCP decode in your frames. You don't care about what has happened at the IP layer or any other layer, so you hide everything but TCP. The window shows just the TCP decode for each frame. With those two steps, you've eliminated looking at any frame that doesn't have TCP in it, and you've narrowed down what you see to just the TCP decode.

7.2.5 Hiding and Revealing Protocol Layers in the Protocol Navigator

Hiding means that the selected protocol is not displayed in the window, even though it may be present in the frame. This allows you to zoom in on a particular protocol by hiding every protocol but the one of interest. This is especially effective when all the layers are expanded.

Note: Hiding affects only the view in the Protocol Navigator and not the view in any other window.

There are two ways to hide a protocol in the Protocol Navigator window :

1. Right-click on the protocol and choose Hide [Protocol Layer Name].
2. There are three panes on the left side of the window. The middle box is the Hidden From View pane. Check the boxes next to the protocols you want to hide.

To reveal a hidden protocol:

1. Right-click anywhere in the main window
2. Select the protocol you want to show from the right-click menu, or un-check the box next to the protocol name in the Hidden From View pane.

When one or more layers are hidden, a note appears at the top of the Protocol Navigator saying, "Some layers are hidden. Right-click to see." This warns you that some layers are hidden.

Two special options are *All But the Last Layer* and *All Special Information Nodes*.

- *All But the Last Layer* hides all layers in each frame except for the last one, regardless of which protocol is present in the last layer.
- *All Special Information Nodes* hides the information line present in some protocol decoders.

7.2.6 Filtering on a Protocol Layer

You can filter on one or more protocol layers. The filter is inclusive which means only frames matching the filter you select are shown in the window. Frames that do not contain the protocol do not appear. You can filter on one protocol or several.

On the left side of the Protocol Navigator window are three panes. The top pane is the Frames Filtered In pane. In the pane is a list of all the protocols seen so far on the circuit.

1. Check the boxes next to the names of the protocols you want to filter in.

The data on the right side of the screen matches the filtering selected.

Three additional filters available are:

- All Frames With Bookmarks - filters in all frames with a *bookmark* associated with them.
- All Frames With Errors - filters in all frames with errors.
- All Special Information Nodes - filters in all *special information nodes* .

7.2.7 Filtering on all Frames with Errors

To filter on all frames with errors :

1. Open the *Protocol Navigator* window.
2. Check the *All Frames With Errors* box in the top pane on the left side of the window.
3. To remove the filter, un-check the box.

7.2.8 Expanding and Collapsing Protocol Layers

You can expand any collapsed frame or protocol layer by clicking on the plus sign next to the frame number or protocol name. Expanding a protocol layer in one frame expands it for all frames.

1. To collapse a layer or frame, click on the minus sign next to the frame number or protocol name.

What do you want to see?

Everything	Choose Show All from the Format menu.
Everything for just one frame	Click the plus sign next to the frame you want to see. Then click the plus signs next to each protocol name to see the full decode.
Just the stack for each frame	Choose Show Frames AND Show Protocol Stack When Frame Is Completely Collapsed from the Format menu. This makes the display look similar to the following:

Frame 1: Len=104 Ethernet -> IP -> TCP

Frame 2: Len=98 Ethernet -> IP -> TCP -> NBSS

Just the stack without summary information	Choose Show Layers AND un-check Show Summary Decode When Detailed Decode Is Collapsed on the Format menu. This makes the display look similar to the following:

Frame 1: Len=104
+ Ethernet:
+ IPv4:
+ TCP:

Frame 2: Len=98
+ Ethernet:
+ IPv4:
+ TCP:
+ NBSS:

Just the stack including summary information

Choose Show Layers AND Show Summary Decode When Detailed Decode Is Collapsed from the Format menu. This makes the display look similar to the following:

Frame 1: Len=104

+ Ethernet: --- Dest. Address: BROADCAST Source Address: XYZ etc.

+ IPv4: --- Protocol: TCP Length: 80 etc.

+ TCP: --- Source Port: 9988 Destination Port: NETBIOS etc.

Frame 2: Len=98

+ Ethernet: --- Dest. Address: etc.

+ IPv4: --- Protocol: TCP Length: 56 etc.

+ TCP: --- Source Port: NETBIOS Destination Port: 9988 etc.

+ NBSS: --- Length: 23 Fragment: Entire Message

The full decode for a protocol layer

Click on the plus sign next to the protocol name. This expands just that protocol in every frame.

The decode for just the last layer in each frame

Choose Collapse All Nodes AND Show Last Layer When Frame is Completely Collapsed from the Tree menu.

8 Statistics

8.1 Statistics Window

The Statistics window supplies basic information about the data on the network. When reviewing a capture file, the Statistics window shows a summary of the data in the file.

To open the Statistics window, click the Statistics icon on the Control window toolbar, or choose Statistics from the View menu on the Control window.

The analyzer monitors the network and collects statistics all the time, even when data is not actively being captured. Activate the Lock icon to stop the window from updating.

Click the Unlock icon again to resume updating. The analyzer continues to monitor network traffic while the Statistics window is locked, so you may see the numbers jump right after updating has resumed, reflecting all the statistics that were gathered while the window was locked.

8.2 Session, Resettable and Capture File Tabs

The Session and Resettable tabs are parts of the Statistics window.

NOTE: This information applies when running FTS4BT in any of the following modes or when viewing a capture file created using any of these modes:

- High Speed Serial HCI
- High Speed UART (HSU)
- USB HCI

Information about all data collected since the analyzer was started is shown in the Session tab. The Session tab cannot be reset; in this sense, it is like the odometer on a car. The odometer on a car shows you all the miles driven since the car was built, and the Session tab shows you all the data collected since the analyzer was started.

If you think of the Session tab as the odometer, then the Resettable tab is the trip odometer. It can be reset, and allows you to record statistics for a new "trip". In this way you can effectively start a new session without having to restart the analyzer. If the Reset button was pressed during the capture, then the numbers on this tab differs from the numbers on the Session tab.

The Capture File tab shows information on the data that is currently in the capture. If the capture file had become full, the analyzer began to overwrite the oldest data and put new data in its place. This is called "wrapping". If the file wrapped, the numbers on the Capture File tab is smaller than those on the Session tab.

Occasionally some of the statistics read n/a, for Not Available. This happens for various reasons. For example, many of the items on the Capture File tab become not available (n/a)

if the buffer becomes full and wraps. When this happens, the analyzer can no longer provide accurate statistics for the data in the file, because some of the data that the statistics are based on has been lost.

8.3 Copying Statistics To The Clipboard

NOTE: This information applies when running FTS4BT in any of the following modes or when viewing a capture file created using any of these modes:

- High Speed Serial HCI
- High Speed UART (HSU)
- USB HCI

To copy the information from an individual table to the clipboard (where it can be pasted into any application),

1. Choose the name of the table from the *Edit* menu.
2. To copy the contents of all the tables, choose *Copy All to Clipboard*.

8.4 Graphs

8.4.1 Statistics Graphs

Open the Statistics window and click on the picture of a graph on the table header, or choose the graph name from the Graph menu on the Statistics window.

The Frame Sizes Graph window has Session, Resettable and Buffer tabs that correspond to the tabs on the Statistics window. Each tab shows the data that corresponds to the appropriate tab on the Statistics window.

The Frame Sizes Graph window displays the number of frames of each length in either a pie chart or bar graph format. Click the Pie icon to display a pie chart, and click the Bar icon to display a bar graph.

For networks with more than one side, the analyzer displays one graph for each side. To view the aggregate of all sides, click the Aggregate icon .

8.4.2 Printing Graphs

1. Click the Print icon to print the graph. The analyzer prints exactly what is shown on the window.

8.4.3 Changing the Graph Refresh Rate

The graphs window refreshes once every second.

To change the refresh rate:

1. Click the Options icon on the *Statistics* window.
2. Enter a new refresh rate in milliseconds in the Time Interval (ms) text box.

8.4.4 Viewing Percentages or Values

On the *Statistics* window you can view data expressed as a percentage.

1. Open the *Statistics* window
2. Select the graph to display.

On the graph window,

3. Click the *Percentages* icon to view data expressed as a percentage.
4. Click the *Percentages* icon again to view the actual number of items of each type.
5. Click the *Show Data Grid* icon to view both the number and percentage of the total for each item. The analyzer places a grid in the legend.

8.5 Information on Tables

8.5.1 Statistics Tables

The Statistics Table is found on the Statistics window. The window displays the following information.

NOTE: This information applies when running FTS4BT in any of the following modes or when viewing a capture file created using any of these modes:

- High Speed Serial HCI
- High Speed UART (HSU)
- USB HCI

The information on the Statistics window is organized into Tables. Fields marked "n/a" are fields for which there is currently no data. This can happen for a variety of reasons. On the buffer tab, fields are n/a when there is no data in the buffer (i.e. no capturing is being done). On the Errors table, some fields may be n/a depending on the statistics supported by your Ethernet card. Some tables are always present, while tables with framing information are present only when capturing framed data.

8.5.2 Bytes Per Second Table

The information in the Bytes Per Second table is recorded while running an Ethernet analysis.

Speed The maximum speed of the network expressed in megabits

Current The current number of bytes per second.

Average The average number of bytes per second.

Peak The highest number of bytes per second.

8.5.3 Frames Per Second Table

The Frames Per Second Table is found on the Statistics window. The window displays the following information.

NOTE: This information applies when running FTS4BT in any of the following modes or when viewing a capture file created using any of these modes:

- High Speed Serial HCI
- High Speed UART (HSU)
- USB HCI

Current The current number of frames per second.

Average The average number of frames per second.

Peak The highest number of frames per second.

The Data Terminal Equipment (DTE) and Data Communication Equipment (DCE) timestamps correspond to the time of the peak utilization.

8.5.4 Utilization Table

The Utilization Table is found on the Statistics window. The window displays the following information.

NOTE: This information applies when running FTS4BT in any of the following modes or when viewing a capture file created using any of these modes:

- High Speed Serial HCI
- High Speed UART (HSU)
- USB HCI

Current The current number of bits per second divided by the maximum speed of the network, expressed as a percentage.

Average The average number of bits per second divided by the maximum speed of the network, expressed as a percentage.

Peak The highest utilization.

The Data Terminal Equipment (DTE) and Data Communication Equipment (DCE) timestamps correspond to the time of the peak utilization.

8.5.5 Data Table

The Data Table is found on the Statistics window. The window displays the following information.

NOTE: This information applies when running FTS4BT in any of the following modes or when viewing a capture file created using any of these modes:

- High Speed Serial HCI
- High Speed UART (HSU)
- USB HCI

The information in the Data table relates to the amount of data captured by the analyzer. Data information varies depending on the type of data in the capture. When Ethernet data passes through a capture filter, this table displays statistics only for the data kept by FTS, i.e. only the data that passes the filter. The Unfiltered Data table always displays statistics for the entire network, regardless of the state of any capture filter.

Ethernet Data

Frames This includes frames received with and without errors, and frames transmitted by the PC running the analyzer, if the PC is an active node on the network. This field and the Total Frames field in the Unfiltered Data table should be roughly equal, unless a capture filter is active. They are not exactly equal because the counters are updated at different times.

Bytes The total number of bytes.

Events The total number of events captured. Events include data bytes and start-of-frame and end-of-frame markers. For a description of all events and their symbols, see the List of Event Symbols.

Multicast The total number of multicast frames.

Broadcast The total number of broadcast frames.

Serial Data

Frames The total number of frames, if applicable, with a breakdown by DTE and DCE device.

Chars The total number of characters, with a breakdown by DTE and DCE device.

Events The total number of events captured. Events include data bytes, control signal changes, flow control changes, etc. For a description of all events and their symbols, see the List of Event Symbols.

Wireless Data

Frames The total number of frames, if applicable, with a breakdown by device.

Octets The total number of octets, with a breakdown by device.

Events The total number of events captured. Events include data bytes, start and end-of-frame markers, etc. For a description of all events and their symbols, see the List of Event Symbols.

8.5.6 Unfiltered Data Table

The information in the Unfiltered Data table is recorded by NDIS while running an Ethernet analysis. Some NDIS drivers may not report all of the statistics on this table, in which case the field lists an n/a. This table always reflects the total amount of data on the network.

Rx Frames W/O Errors The total number of frames received with no errors.

Tx Frames W/O Errors The total number of frames transmitted by the NIC with no errors.

Total Frames The total number of frames, including frames with errors. This field and the Frames field on the Data table should be roughly equal, unless a capture filter is active. They are exactly equal because the counters are updated at different times.

Bytes The total number of bytes.

Multicast Frames The total number of multicast frames.

Broadcast Frames The total number of broadcast frames.

8.5.7 Buffer Information Table

NOTE: This information applies when running FTS4BT in any of the following modes or when viewing a capture file created using any of these modes:

- High Speed Serial HCI
- High Speed UART (HSU)
- USB HCI

These errors do not indicate problems on the network, but rather indicate that FTS was not able to keep up with the amount of incoming data. They usually indicate that a faster PC was needed. See Performance Notes for more information.

Driver Buffer Overflow — The number of times the analyzer lost frames because it could not retrieve them from the driver buffer fast enough.

The remaining three items are for Ethernet data only.

Frames Missed, No Buffer — The number of frames lost because the analyzer driver could not retrieve them from the NDIS buffers before they were overwritten by new, incoming frames.

Receive Overrun — The number of times that frames are lost because NDIS could not retrieve data quickly enough from the buffer on the network card.

Frames Lost — The number of frames lost due to driver buffer overflows.

8.5.8 Errors Table

The Errors Table is found on the Statistics window. The table provides the number of each type of error seen on the network. Error types vary depending on the type of data. When analyzing Ethernet data, not all errors are supported by all NDIS drivers. Errors not supported are marked "n/a".

NOTE: This information applies when running FTS4BT in any of the following modes or when viewing a capture file created using any of these modes:

- Serial Asynchronous
- High Speed Serial HCI
- High Speed UART (HSU)

To graph, click the bar graph icon on the Errors table header.

Ethernet Errors

CRC Errors	The number of frames with *CRC* errors. A CRC error occurs when the frame is properly aligned on a byte boundary but does not pass the Cyclic Redundancy Check. The CRC verifies that the data was not corrupted in transit.
Alignment Errors	The number of frames with alignment errors. Alignment errors occur when the frame does not end on a byte boundary. For example, frames may not be 95 and 2 bits long. It must be either 92 or 93 bytes.
Rx Frames With Errors	The total number of frames received with errors (includes frames with CRC and Alignment errors).
Tx Frames With Errors	The total number of frames transmitted with errors.
Tx One Collision	The number of frames successfully transmitted after detecting one collision.
Tx More Collisions	The number of frames successfully transmitted after detecting multiple collisions.
Tx Deferred	The number of frames successfully transmitted after transmission has been deferred at least once.
Tx Max Collisions	The number of frames not transmitted due to excessive collisions.
Tx Underrun	The number of frames not transmitted due to underrun errors.
Tx Heartbeat Failure	The number of frames transmitted without detecting the collision detection heartbeat.
Tx Times CRS Lost	The number of times carrier sense was lost during frame transmission.
Tx Late Collisions	The number of collisions detected after the normal window.

Serial Asynchronous Errors

Overrun The number of overrun errors broken down by DTE and DCE device.

Parity The number of parity errors broken down by DTE and DCE device. If you have a large number of parity errors, check your I/O Settings for accuracy.

Framing The number of framing errors broken down by DTE and DCE device. If you have a large number of framing errors, check your I/O Settings for accuracy.

Serial Synchronous Errors

USART Overrun The number of overrun errors broken down by DTE and DCE device.

Parity The number of parity errors broken down by DTE and DCE device. If you have a large number of parity errors, check your I/O Settings for accuracy.

Framing The number of framing errors broken down by DTE and DCE device. If you have a large number of framing errors, check your I/O Settings for accuracy.

CRC The number of *CRC* errors detected. CRC counting is done only when monitoring HDLC or SDLC data.

Underrun The number of underrun errors broken down by DTE and DCE device. Underrun errors occur when FTS is unable to transmit data quickly enough. These errors only occur when transmitting in sync mode.

High Speed Serial HCI and High Speed UART (HSU) Errors

Parity The number of parity errors broken down by device.

Framing The number of framing errors broken down by device.

ZigBee Errors

FCS The number of FCS errors detected.

9 Network View

9.1 Network View Introduction

The Network View is a graphic depiction of network nodes and connections between them as indicated by packets received by the analyzer. Information shown includes node statistics, node addresses and names, node pair (i.e. conversation) statistics, and network statistics.

Access the Network View either by selecting *Network View* from one of the *View* menus on other dialogs or by pressing the *Network View* icon on one of the other dialogs.

The Network View consists of the following dialogs:

- The main Network View dialog
- A Node Database dialog
- An Edit Alias dialog
- A Set Count For Top N Filter dialog

For more information on the Network View, see Network View Technical Notes

9.2 Display Node Information in Network View

The user has complete freedom to specify as many or as few statistics, addresses, and names as are desired and in whatever order is desired. There are ten statistics selections and six name/address selections available for display with each node. Selections to display or remove node information can be made using one of the menus at the top of the dialog (Statistics, Addresses, and Names), or by selecting icons in the toolbar. Select *Show Lines and Dots Only* from the *Format* or right-click menu to hide all node and conversation information in the Detail window, and select it again to display information.

Display:

- Node Statistics

  To display a node statistic in the Detail window, simply select the statistic from the *Statistics* menu or select the appropriate icon from the toolbar. The selected statistic appears at the bottom of the upper list associated with each node in the Detail window. When a statistic is selected, its associated icon appears depressed and its menu item is checked. To remove the statistic from the display, simply select it again. To place the statistic at the top of the node list, press and hold the Ctrl key while selecting the statistic.

  Select from among the following:

  - Bytes Received (BR)
  - Bytes Sent (BS)

- Bytes Total (BT)
- Nodes In (NI)
- Nodes Out (NO)
- Nodes Total (NT)
- Packets Received (PR)
- Packets Sent (PS)
- Packets Total (PT)
- Utilization (UT)
- Show All Conversations
- Hide All Conversations
- Show Visible Conversations as Bytes (CB)
- Show Visible Conversations as Packets (CB)
- Hide Zero Count Statistics

- Node Addresses

  To display a node address in the Detail window, simply select the address from the *Address* menu or select the appropriate icon from the toolbar. The selected address appears at the bottom of the lower list associated with each node in the Detail window. When an address is selected, its associated icon appears depressed and its menu item is checked. To remove the address from the display, simply select it again. To place the address at the top of the node list, press and hold the Ctrl key while selecting the address.

  Select from among the following:

  - IP Address (IP)
  - MAC Address (MC)
  - Named MAC Address (NM)
  - Order of Appearance
  - Hide Empty Addresses and Names

- Node Names

  To display a node name in the Detail window, simply select the name from the *Names* menu or select the appropriate icon from the toolbar. The selected name appears at the bottom of the lower list associated with each node in the Detail window. When a name is selected, its associated icon appears depressed and its menu item is checked. To remove the name from the display, simply select it again. To place the address at the top of the node list, press and hold the Ctrl key while selecting the name.

  Select from among the following:

  - Alias (AL)
  - DNS Name (DN)

- NetBIOS Name (NB)
- Automatically Resolve IP to DNS - You must select this option to use the **Show DNS Names** on the Dashboard
- Hide Empty Addresses and Names

- Node Information Display Options

  In addition to the individual selection options described above, you have several other options for displaying information using the Format menu:

  - Display all node information by selecting *Show All Node Info*
  - Hide all by selecting *Hide All Node Info icon*
  - *Restore Node Info* to return the display to its original state

For a list of node information selections and their corresponding toolbar icons see Network View Toolbar.

9.3 Displaying Conversation Information in Network View

Conversation Statistics

Conversation statistics display on the lines between nodes.

1. Select *Show Info for All Conversations* from the *Format* or right-click menu, or simply click the toolbar icon .
2. Choose the units to display by selecting *Show Visible Conversation as Bytes* or *Show Visible Conversation as Packets* from the *Statistics* menu..
3. In the event that the Detail window becomes crowded, the conversation statistics may become hidden behind the node statistics display.
4. Select *Put Lines and Conversations On Top* from the *Format* or right-click menu, or click the icon on the toolbar.
5. Select the menu item again or click the toolbar icon to place the conversation statistics in the background.
6. To hide all conversation statistics, select *Hide Info for All Conversations* from the *Format* or right-click menu, or simply click on the toolbar.

Quick Tip:

To view statistics for a subset of conversations

- Hover the mouse pointer over the desired node conversation to highlight the line (the line turns magenta to indicate selection)
- Right-click and select *Show this Conversation*.
- Select the menu item again to hide the conversation statistics.

9.4 Adding/Editing an Alias for a Node in Network View

Specifying aliases

An alias is an arbitrary string up to 200 characters in length that the user can define and associate with any MAC address. Each MAC address can have a different alias. Aliases are remembered between sessions and apply to all live captures and capture files. Each alias takes effect as soon as the *OK* button is pressed on the Edit Alias dialog. The Node Database dialog has a Freeze button so that aliases can be added without the dialog's entries moving around.

Add/Edit an Alias

1. Click the *Node Database* icon or select *Node Database* from the *View* menu on the Network View dialog to open the Node Database dialog.
2. Select the row containing the alias you want to add/edit and click the *Edit Alias* button (or simply double click the row) to open the Edit Alias dialog. (Note that during live capture, entries in the Node Database may be moving around, which can make it difficult to select the entry you want. Simply click the *Freeze* button to freeze the display, then click the *Unfreeze button* when you are finished.)
3. Add/edit the alias in the text box and click *OK*.
4. Repeat steps 2 and 3 until all aliases you want to change are completed, and close the Node Database dialog.

Quick Tip:

If you need only add/edit one alias, then hover the mouse pointer over the desired node in the Detail window, right click, and select *Edit Alias* from the menu to open the Edit Alias dialog.

9.5 Filter and Sort the Network View

Filtering:

The *Filter* menu and the tabs above the detail window set the current filter. The filter is always applied to the current sort. Changing the sort criterion may change which nodes are filtered in and which are filtered out.

- **Unfiltered**

  Shows all nodes.

- **No Broadcasts**

  Hides the broadcast node and its conversation lines (i.e. the orange dot and all orange lines disappear).

- **Top N [*Sort by* selection]**

  This shows the top N nodes or conversations based on the statistic listed on the tab (the current sort). The "N" value defaults to 10, but can be set to any value.

- **Top N [*Sort by* selection], No Broadcasts**

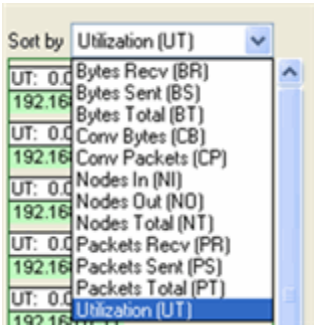
Hides the broadcast node and its conversation lines, then displays the top N of the remaining nodes or conversations based on the statistic listed on the tab (the current sort). The value of N is the same value used in the Top N filter.

- **Always Shown**

  This shows all nodes that have been marked via the right-click menu as being always shown. The right-click menu makes it possible to specify that the current node, the current node pair (if the mouse cursor is on a conversation line), or all currently selected nodes always be shown (those selected nodes retain this attribute even after they're unselected). The *Undo "Always Shown" For All Nodes* icon in the toolbar, along with selections in the right-click and *Format* menus, removes this attribute from all nodes. Marking a node as always shown not only ensures that it is always visible regardless of which filter is in effect (inclusion mode), but also makes it possible to isolate nodes by clicking on the Always Shown tab (isolation mode). When a node is visible solely because it's always shown, a little white dot is drawn in the center of it. Thus an always shown node is always visible when the top N filter is in effect, but only when it is not in the top N does it contain a white inner dot. In this way a node's statistics and whether it is in the top N can be monitored simultaneously.

Sorting:

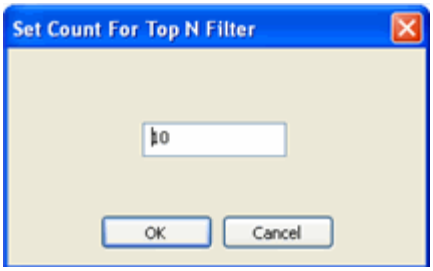
In the Network View, one sort or another is always in effect. Select the statistic to sort on from the *Sort by* drop-down box above the Statistics Graph. The sort in effect is displayed on the Top N tabs and in the Statistics Graph in descending order. The sort order determines which nodes appear in the Detail window when one of the Top N filters is applied.



9.6 Setting The Count For Top N Filters

The Set Count for Top N Filters is an option on the Network View.

1. Click the *Set Count For Top N Filter* icon , or select *Set Count For Top N Filter* from the *Format* menu to display the Set Count For Top N Filter dialog.



2. Enter a new value for N and click *OK*.

The new value of N appears on the Top N filter tabs on the Detail window.

9.7 Detail Window Layouts in Network View

There are three layout possibilities for the Detail window, each of which provides a different degree of flexibility. Layouts are selected from the Format menu or by selecting icons on the toolbar. Select *Use Black Background* from the *Format* or right-click menu to display a black background in the Detail window.

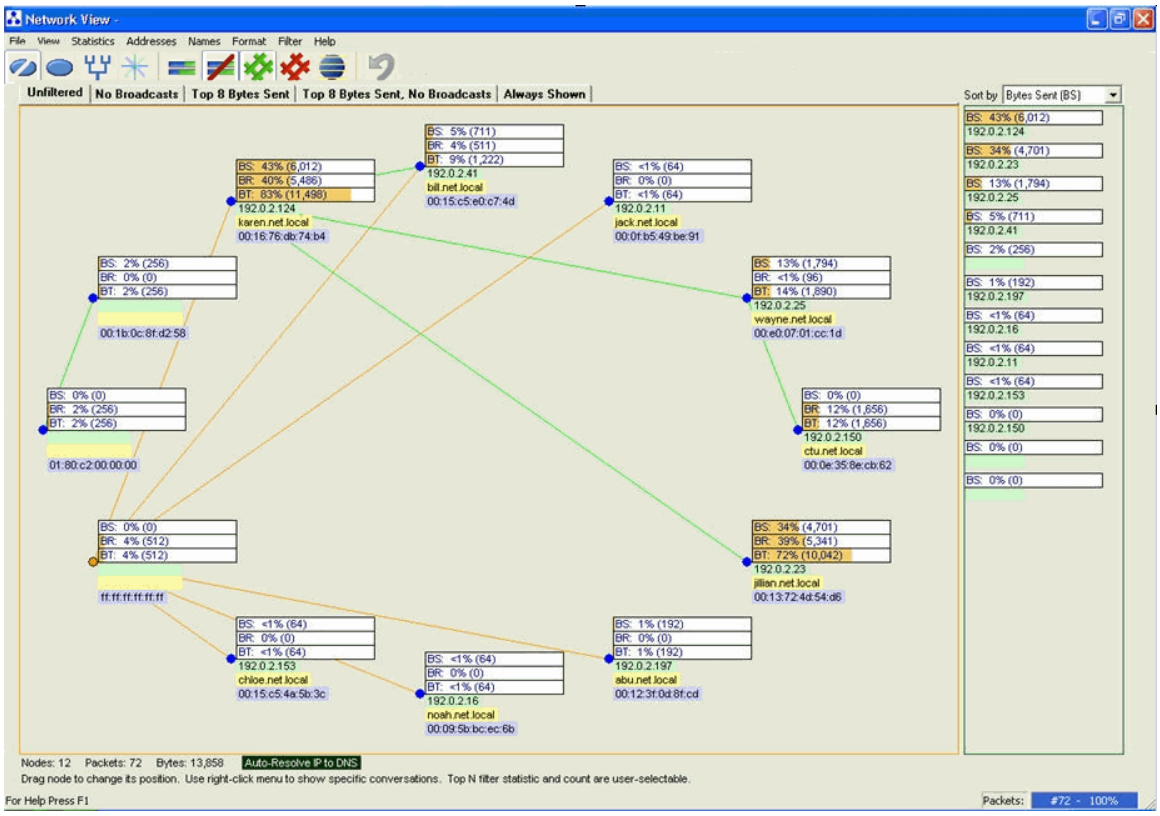
- **Exploded Oval Layout**

  Exploded Oval Layout shows nodes evenly arranged in an oval shape in the Detail window. Click the *Exploded Oval Layout* icon or select *Exploded Oval Layout* from the *Format* menu to display this layout.

- **Oval Layout**

  Oval Layout also shows nodes in an oval, but instead of arranging them evenly around the oval it leaves gaps where nodes have been filtered out. Since nodes don't move (except for the slight rotation around the oval that occurs each time a new node is discovered and added), this makes it easy to see nodes appear and disappear as they are filtered in and out. On the other hand, it can be more congested than Exploded Oval Layout and thus harder to read. Click the *Oval Layout* icon or select *Oval Layout* from the *Format* menu to display this layout.

Network View Main Dialog with Oval Layout:

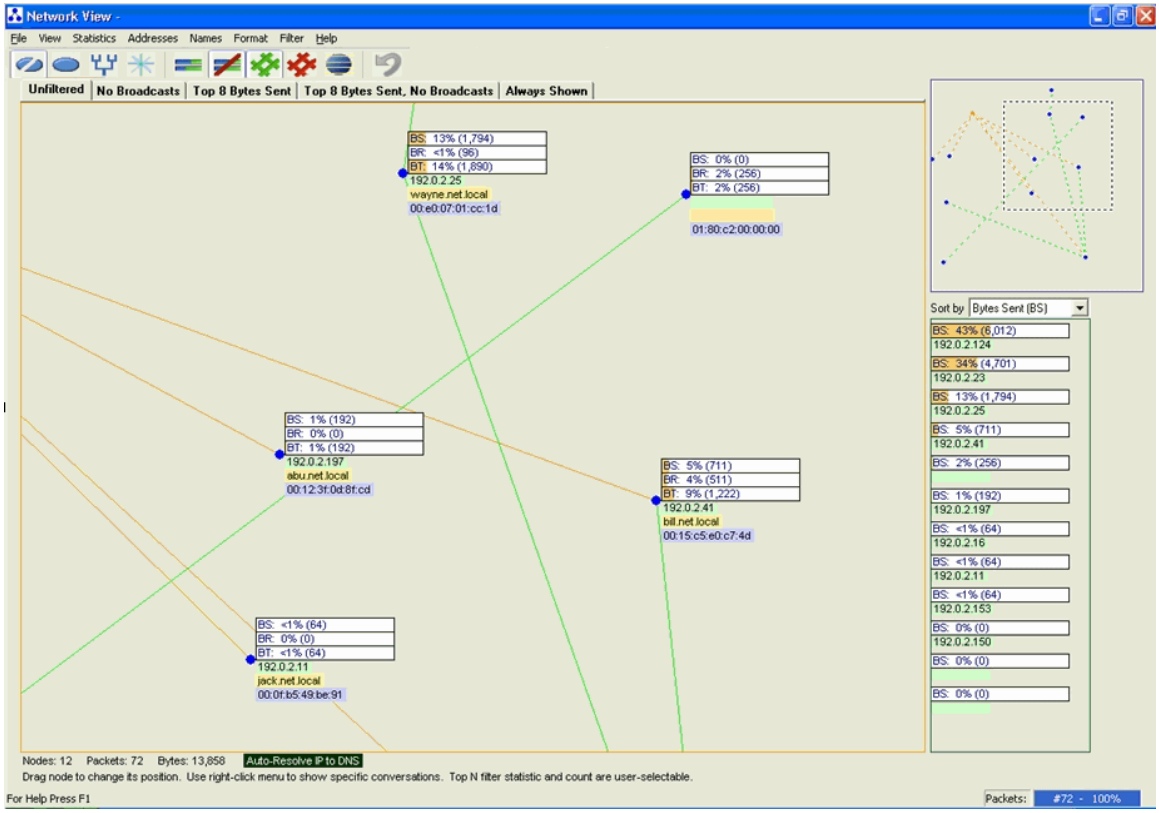


Both Exploded Oval Layout and Oval Layout leave gaps for nodes that the user has dragged (see *Positioning Nodes in the Detail Window* below). In both of those layouts, the oldest node is at the far right and halfway up the detail window (i.e. at the 3 o'clock position). The next oldest node is just above it, and the newest node is just below it. When a node appears for the first time, it is placed just below the oldest node, and the other nodes rotate clockwise around the oval.

- **Branched Layout**

  Branched Layout shows nodes in a free format, and also shows an Overview window which contains a zoomable and movable viewport that can be used to focus the Detail window on a specific area of the network. Branched Layout assigns node positions randomly. Click the *Branched Layout* icon or select *Branched Layout* from the *Format* menu to display this layout.

Network View Main Dialog with Branched Layout:



Positioning Nodes in the Detail Window

- **Oval Layouts**

  Nodes can be selected and dragged in either Oval layout. A dragged node is not auto-located in either of the Oval layouts, so it provides a means in those layouts for a user to freeze the position of a node. Nodes can be dragged singly or in groups. Select multiple nodes either by using Ctrl-click or by enclosing desired nodes in a box created by dragging the mouse. Simply click in any vacant area of the Detail window to de-select. Dragged nodes can be moved back into the oval of the current Oval layout by clicking the *Move Dragged Nodes Back Into Oval* icon or by selecting *Move Dragged Nodes Back Into Oval* from the *Format* menu.

- **Branched Layout**

  Nodes can be selected and dragged in the Branched layout. Nodes can be dragged singly or in groups. Select multiple nodes either by using Ctrl-click or by enclosing desired nodes in a box created by dragging the mouse. Simply click in any vacant area of the Detail window to de-select. To see any nodes that have been dragged outside of the Detail window, select *Reformat Branched Layout* from the *Format* menu to re-position all nodes within the window.

9.8 The Statistics Graph Window in Network View

The Statistics Graph window displays, in list format, a subset of the node or conversation information displayed in the Detail window. This window is always sorted in descending order of the statistic displayed. The statistic that appears in this window can be one of ten Node statistics, or one of two Conversation statistics, and is user controlled.

- **Node Statistics**

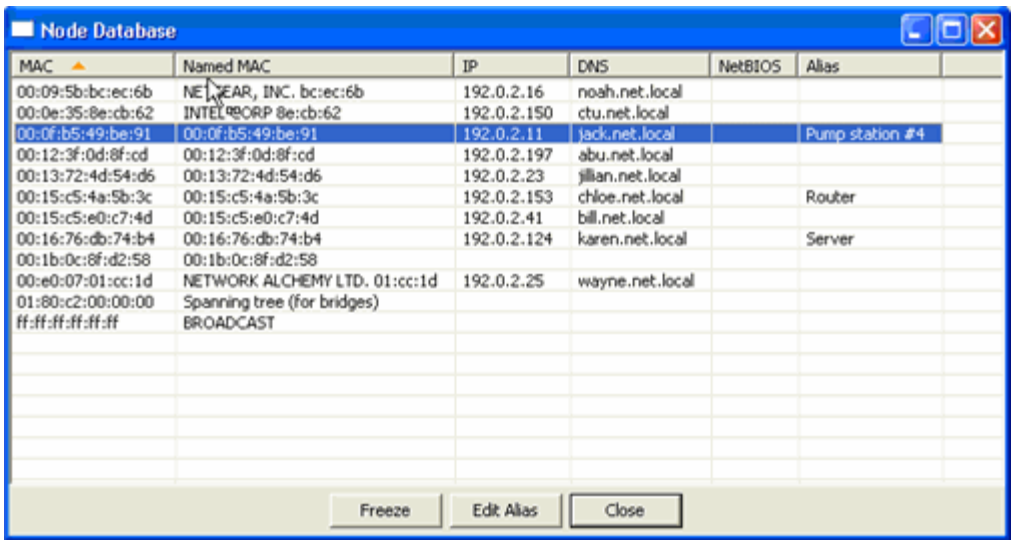
  When a node statistic is chosen as the sort criterion, the Statistics Graph displays the selected statistic and the topmost address/name (as it appear in the Detail window) for each node displayed in the Detail window. The statistic line for each node displays the abbreviation of the selected statistic, its percent value, and its actual value. The only exception is Utilization, where only the actual value is displayed. The statistics line also functions as a bar graph that displays the percent value of the statistic from left to right. This list sorts in descending order and has scroll capability.

- **Conversation Statistics**

  When either Conversation Bytes (CB) or Conversation Packets (CP) statistic is chosen as the sort criterion, the Statistics Graph displays the selected conversation statistic, and the topmost addresses/names (as they appear in the Detail window) for the corresponding pair of nodes displayed in the Detail window. The statistic line for each node displays the abbreviation of the selected conversation statistic (CB or CP), its percent value, and its actual value. The statistics line also functions as a bar graph that displays the percent value of the statistic from left to right. This list sorts in descending order and has scroll capability.

9.9 The Network View Node Database

The Node Database dialog shows node addresses and names in a sortable table. It is kept up-to-date with the Network View main dialog at all times unless the Freeze button on the Node Database dialog has been pressed, in which case no new rows are added (individual fields within each entry are still updated however). The purpose of the Freeze button is to keep the table entries in one place while the user is in the process of adding aliases. The display can be sorted on any column in ascending or descending order simply by clicking on the column header. The sort in effect, and the direction of the sort, is indicated by a pointer in the column header. The sorted column is sorted such that blank entries always appear at the bottom of the column.



9.10 Resolving DNS Names in Network View

IP addresses are resolved to DNS names in two ways: automatically or manually. Resolution is achieved via network query, and is the only instance in which the Network View places a message on the network. In auto-mode, at most one resolution is attempted per second to ensure that Network View-generated traffic is minimal. Other processing continues while this resolution is underway.

- **Resolve DNS Names Automatically for All IP Addresses**

  Select *Automatically Resolve IP To DNS* from the *Names* menu or from the right-click menu.

  A check mark appears next to the menu item and the text *Auto-Resolve IP to DNS* appears in the Status line just below the Detail window.

  To stop auto-resolve, simply select (un-check) the menu item again.

- **Resolve DNS Names Manually for Individual IP Addresses**

  If you need only resolve one or two IP addresses, then hover the mouse cursor over the desired node in the Detail window and select *Resolve IP to DNS* from the right-click menu. Once resolution is complete, the DNS for the selected node appears in the node's list (ensure that DNS Name is selected as a list item).

9.11 The Network View Toolbar

The toolbar contains the following:

Exploded Oval Layout - Displays the Exploded Oval Layout in the Detail window

Oval Layout - Displays the Oval Layout in the Detail window

Branched Layout - Displays the Branched Layout in the Detail window

Move Dragged Nodes Back Into Oval - Moves any nodes that were dragged from their original positions back to those positions.

Show All Conversations - Shows all conversation statistics in the Detail window.

Hide All Conversations - Hides all conversation statistics in the Detail window.

Put Lines and Conversations On Top - Displays lines and conversation statistics on top of nodes and node information (statistics, addresses, and names) in the Detail window.

Undo Always Shown For All Nodes icon - Removes the *Always Shown* attribute from all nodes.

9.12 Network View Visual Elements

The main Network View dialog consists of the following visual elements:

- **The Title Bar**

  The Title Bar shows the name of the current capture file (if any).

- **The Menu Bar**

  The Menu Bar contains pull-down menus with selections for all functions in Network View.

  - File - Allows you to hide/show the Toolbar and Status bar, and also Exit
  - View - Allows you to open the Dashboard, Frame Sizes, and Node Database dialogs
  - Statistics - Allows you to activate/deactivate various statistics
  - Addresses - Allows you to hide/show various address types
  - Names - Allows you to hide/show various name types
  - Format - Allows you to choose between Exploded, Oval, and Branched layouts. Also allows you to hide/show types of data.
  - Filter - Allows you to manage the type and amount of information displayed.
  - Help - Opens the Help files

- **The Toolbar**

The Toolbar contains buttons for display selection, and frequently used functions.

- **The Detail Window**

  The Detail window displays each node, connections between nodes, various user-selectable statistics and addresses, and mouse hover information windows (aka tooltips). This window has a set of tabs just above it which provide filter selection.

- **The Statistics Graph Window**

  The Statistics Graph window displays a subset of the node information that is displayed in the Detail window in list format. This window displays the statistic selected in the *Sort by* drop-down box located at the top of the window. The Statistics Graph window lists the selected statistic in descending order, along with the topmost Name/Address (as it is displayed in the Detail window).

- **The Overview Window**

  The Overview window provides the ability to scroll and zoom the spatially oriented Branched Layout in the Detail window, and display all or part of the network

  Note: This window appears only in Branched Layout.

- **The Status Line**

  The Status Line appears just below the Detail window, and displays various totals and states.

- **The Instruction Line**

  The Instruction line appears just below the status line, and contains some simple instructions for the user.

The Network View dialog is re-sizable and contains a right-click menu. The “Packets” indicator in the lower-right corner is identical to those on the Control Window and Frame Display.

9.13 Network View Technical Notes

Information Gathering and Processing

- Packets are used to obtain addresses and compute statistics for each node, each pair of connected nodes, and for the network as a whole.
- System query is used to resolve IP addresses to DNS names.
- Aliases are specified by the user.
- Node statistics are saved for each occurrence of each MAC address in each packet. A complete list of node and conversation statistics is given in a table below.

- Conversation statistics are saved for each pair of MAC addresses from each packet, and is direction-specific.
- Network statistics are simply a total of all of the node statistics.
- Since statistics are saved by MAC address, a changing IP address does not change the computed statistics.

Information Storage

The obtained and computed information is saved when a live capture is saved to a capture file. When the capture file is reopened, the stored information is retrieved and used without having to reprocess the packets in the capture file.

Textual and Graphical Representation

Each node is represented as a dot, and one or more conversations between a pair of nodes are indicated by a single line connecting the two corresponding dots. Dots are normally blue and lines are normally green, but broadcasts are shown as orange lines that are connected to a single orange dot that does not represent an actual node and whose sole purpose is to provide a broadcast endpoint.

Node statistics, addresses, and names are displayed to the right of each node in the Detail window. Statistics are displayed above the centerline of the dot that represents the node. Addresses and names are displayed below the centerline.

With the exception of utilization, each statistic is displayed as a little horizontal single-item bar graph which shows the count and percentage as text and uses the bar to graphically represent the percentage. A text prefix and text color-coding indicate which statistic it is (see table below).

Utilization does not show a percentage. Instead, it uses color-coding to indicate its absolute value (see table below).

Addresses and names have color-coded backgrounds: MAC = purple, Named MAC = cyan, IP = light green, DNS = yellow, NetBIOS = blue, and Alias = light red.

There can be any number of statistics, addresses, and names displayed for each node, and these are selected via the icons in the toolbar at the top of the main Network View dialog. The order of display follows the order of selection from top to bottom, except that selecting an icon via a Ctrl-click puts that item at the top of the list instead of at the bottom.

Node or conversation data is displayed in the Statistics Graph depending on the selection made in the *Sort by* combo box above the graph. The entries in the Statistics Graph are sorted by descending statistic value.

Conversation data is displayed along each line that connects two nodes and is direction-specific. Either byte count or packet count can be displayed (this is done via the Format menu, right-click menu, or by selecting the Conversation Bytes or Conversation Packets icons in the toolbar). These statistics are displayed as single-item bar graphs which always hug the line connecting the nodes, rotating as the line is rotated. The statistic text flips as the user moves the line through vertical so that the text is never upside-down. A little arrow at the end of the statistics box indicates the direction of the conversation. The colors in a conversation statistic bar graph (green on blue) are different from the colors in a node statistic bar graph (orange on white) so that it's easy to distinguish between them.

User Defined Settings

User defined settings and display options listed below persist across sessions.

- Layout selection
- Positions of dragged nodes in Oval Layout and Exploded Oval Layout
- Positions of all nodes in Branched Layout
- Filter selection
- *Count for Top N Filter* setting
- Sort order selection
- *Always Shown* node selections
- Node statistics, addresses, and names selected for display
- Conversations displayed and statistic selected
- *Put Lines and Conversations On Top* selection
- Detail window background color selection
- *Show Lines And Dots Only* selection
- Auto-resolve IP addresses to DNS names selection
- Aliases

Node and Conversation Statistics:

Prefix	Type	Bar Graph?	Text Color	Bar Graph Color	Description
BR	Node	Yes	Blue	Orange on White	Bytes Received
BS	Node	Yes	Blue	Orange on White	Bytes Sent
BT*	Node	Yes	Blue	Orange on White	Bytes Total (Bytes Received + Bytes Sent)
NI	Node	Yes	Green	Orange on White	Nodes In
NO	Node	Yes	Green	Orange on White	Nodes Out
NT**	Node	Yes	Green	Orange on White	Nodes Total

PR	Node	Yes	Red	Orange on White	Packets Received
PS	Node	Yes	Red	Orange on White	Packets Sent
PT*	Node	Yes	Red	Orange on White	Packets Total (Packets Received + Packets Sent)
UT	Node	No	See following table	See following table	Utilization (Megabits/Sec over the last 10 seconds, counting both Bytes Sent and Bytes Received)
CB	Conversation	Yes	Blue	Green on Blue	Conversation Bytes
CP	Conversation	Yes	Red	Green on Blue	Conversation Packets

**The Bytes Total and Packets Total statistics each add up to 200% since they count each byte twice, once at the sending node and once at the receiving node.*

*** The Nodes Total statistic counts unique nodes, so it's not simply a sum of nodes sent to and nodes received from. For example if node A sends to only nodes B and C and receives from only node B, its total node count is 2, not 3.*

Here is utilization coloring:

Utilization (Megabits/Second)	**Colors**
<0.01	Black on White
>= 0.01 and < 2	White on Dark Blue
>= 2 and < 3	Black on Yellow
>= 3	White on Dark Red

Utilization for each node is shown as megabits/second and is computed over the last 10 seconds, even if the node has been present for less time than that. Both bytes sent and bytes received are counted, so if there are only two devices A and B on the network and all that is

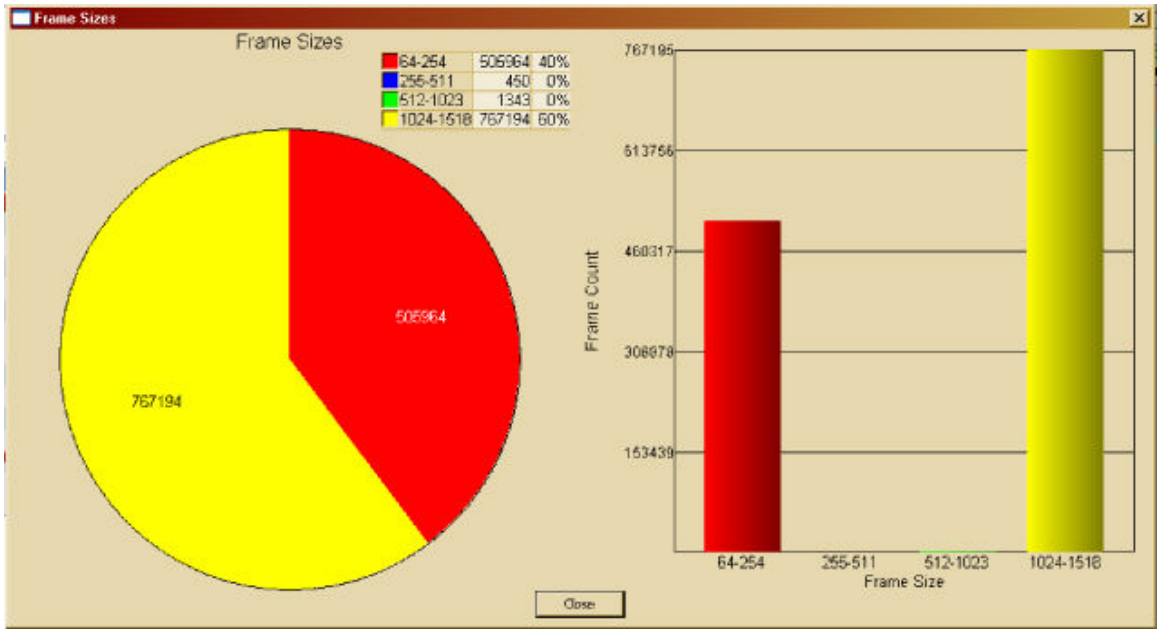
happening is that device A is sending to device B, both of those devices display the same utilization.

A mouse hover information window (aka tooltip) showing all statistics, addresses, and names can be displayed for each node. The tooltip background is normally yellow, but since the nodes can move, the tooltip background turns green and the text "*** Node not under mouse pointer" appears at the bottom of the tooltip when the node moves out from under the mouse pointer or disappears altogether. The tooltip itself, however, persists until the user moves the mouse pointer or presses Esc. The tooltip regains its original yellow appearance if the node moves back under the mouse pointer.

9.14 Network View - Frame Sizes

The Frame Sizes window is accessed from the Network View > View menu.

The window displays the percentage of captured data in four byte size ranges: **64-0254**, **255-511**, **512-1023**, and **1024-1518** in a pie chart and a vertical graph.



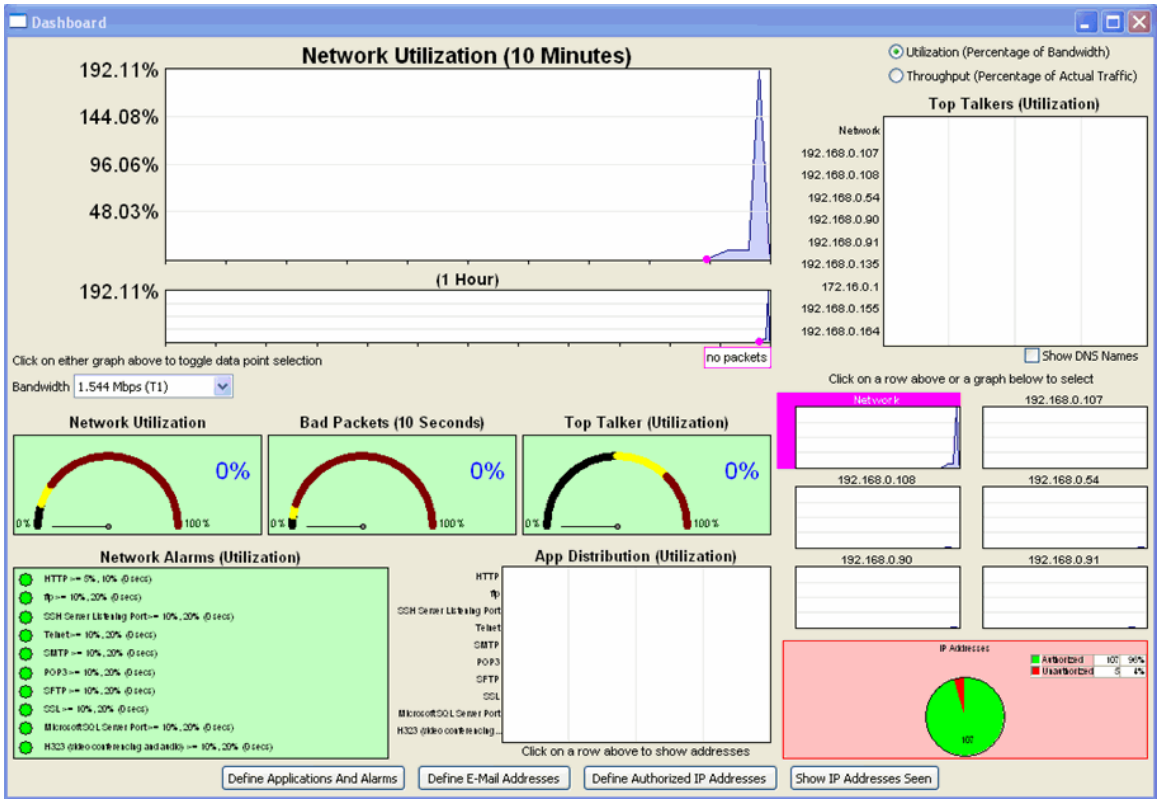
The window is a display only. There is no user interaction.

10 NetDecoder Dashboard

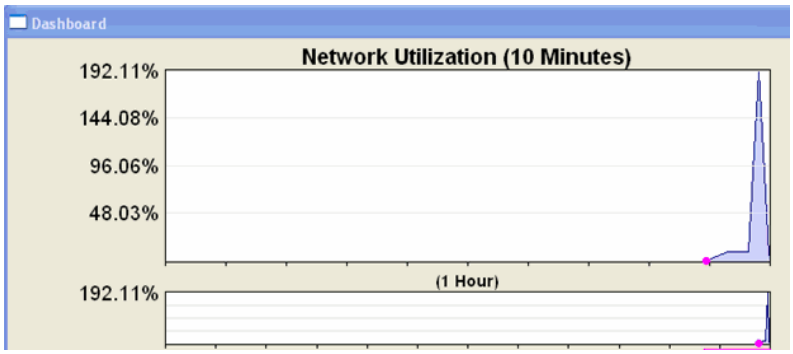
10.1 Dashboard

The Dashboard View displays a dynamic view of what is occurring on your Ethernet communications network.

You access the Dashboard by selecting Dashboard from the View Menu on the Control Toolbar and Network View windows or from the Dashboard icon on the Control Window and Frame Display Toolbars.



10.1.1 One Hour/Ten Minute Chart

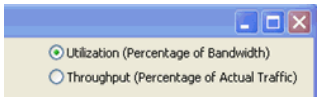


These graphs displays the activity for the last one (1) hour/ten minutes for an IPaddress or DNS Name selected on the Top Talkers (Utilization) or Top Talkers (Throughput) bar chart. Clicking on an IP address in the chart changes the graph.

A pink dot appears when you click on the bottom of the graph. The dot synchronizes between the One Hour/Ten Minutes charts..

A black dot appears when you select a point on the graphs.

10.1.2 Dashboard: Utilization (Percentage of Bandwidth) and Throughput (Percentage of Actual Traffic)



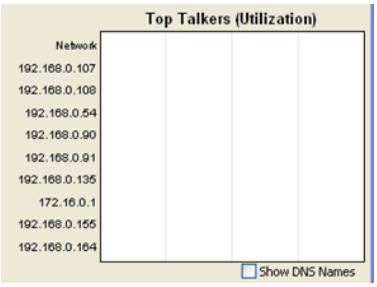
On the Dashboard, selecting the **Utilization (Percentage of Bandwidth)** button affects several areas of the Dashboard:

- Top Talkers Utilization/Top Talkers Throughput Graph - Displays utilization expressed as % bandwidth. Shows for network and each device in descending order. Max 10 entries.
- Bad Packets (10 Seconds)/Bad Packets Meter - Displays % bad packets over last 10 seconds.
- Top Talker Utilization/ Top Talker (Throughput) - Displays utilization expressed as % bandwidth for device with highest utilization.
- Application Distribution Utilization/Application Distribution (Throughput) - Displays utilization expressed as % max bandwidth per specified app for last 10 seconds or since app was defined, whichever is less. Show apps in definition order.

Selecting **Throughput (Percentage of Actual Traffic)** affects several areas of the Dashboard:

- Top Talkers Utilization/Top Talkers Throughput Graph - Displays bytes sent since beginning of session of each device in descending order. Max 10 entries.
- Bad Packets (10 Seconds)/Bad Packets Meter - Displays %bad packets since beginning of session.
- Top Talker Utilization/ Top Talker (Throughput) - Displays percentage of bytes sent since beginning of session for device with highest bytes sent count.
- Application Distribution Utilization/Application Distribution (Throughput) – Displays percentage of bytes sent and received since the app was defined. Shows the apps in definition order.

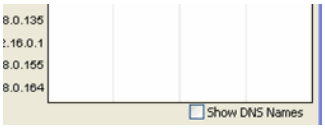
10.1.3 Top Talkers Bar Chart



This bar chart displays bytes sent since beginning of session of each device in descending order with a maximum of 10 entries when the Throughput (Percentage of Actual Traffic) radio button is selected.

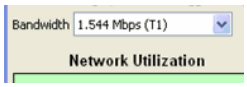
The chart displays utilization expressed as % bandwidth with a maximum of 10 entries when the Utilization (Percentage of Bandwidth) radio button is selected.

10.1.4 Show DNS Names



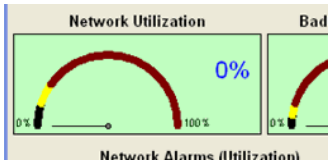
Selecting the Show DNS Names checkbox changes the IP Address displayed in the Top Talkers (Utilization)/Top talkers (Throughput) bar chart to a DNS name. If the DNS name is not available, the IP address is displayed. In order for the DNS name to be available, you must activate Automatically Resolve IP to DNS from the Names menu on the Network View.

10.1.5 Bandwidth Drop-down



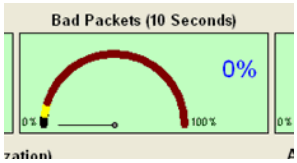
With the drop-down box you can select to view the maximum bandwidth of 1 Gigabyte per second (1 Gbps), OC-3 (155 megabits per second), 100 megabytes per second (100 Mbps), T-3 (43.232 megabits per second), 10 megabytes per second (10 Mbps), and T-1 (1.544 megabits per second).

10.1.6 Network Utilization Meter



Displays the utilization of all devices expressed as % of bandwidth

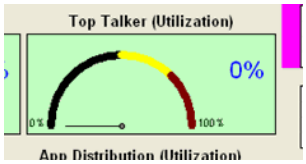
10.1.7 Bad Packets Meter



The Bad Packets (10 Seconds)/Bad Packets Meter displays two different sets of data depending on whether the Percentage of Max Utilization radio button or Percentage of Bytes radio button is selected.

- Utilization (Percentage of Bandwidth) - Displays the % bad packets over last 10 seconds.
- Throughput (Percentage of Actual Traffic) - Displays the % bad packets since the beginning the session.

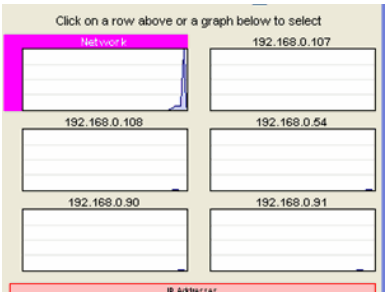
10.1.8 % Top Utilization/Top Utilizer Meter



The Top Talker (Utilization)/Top Talker (Throughput) displays two different sets of data depending on whether the Utilization (Percentage of Bandwidth) radio button or Throughput (Percentage of Actual Traffic) radio button is selected.

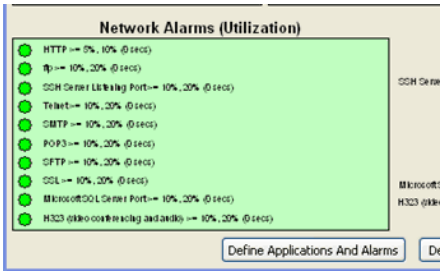
- Top Talker (Utilization) - Shows utilization expressed as % of bandwidth for device with highest utilization.
- Throughput (Percentage of Actual Traffic) - Shows percentage of bytes sent since beginning of session for device with highest bytes sent count.

10.1.9 Charts



These charts displays the Network and top five Top Talkers or Top Utilization IP Addresses from the chart directly above.

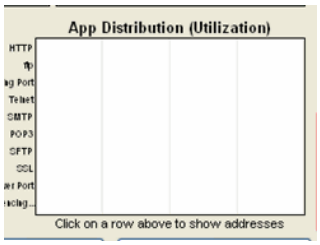
10.1.10 Network Alarms (Utilization)



This chart displays the network alarms configured in the Define Applications and Alarms (Utilization).

- If the data does not exceed the alarms configuration, the tables displays green.
- If the data equals or exceeds the Yellow threshold level, the Network Alarms (Utilization) table displays yellow and an e-mail is sent to each e-mail address specified in the Define E-Mail Addresses dialog.
- If the data equals or exceeds the Red threshold level, the Network Alarms (Utilization) table displays red and an e-mail is sent to each e-mail address specified in the Define E-Mail Addresses dialog.

10.1.11 App Distribution (Utilization/Throughput)

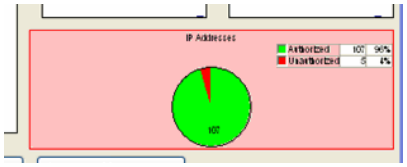


When you select Utilization (Percentage of Bandwidth) radio button, the chart displays the utilization expressed as % bandwidth per specified app for last 10 seconds or since the app was defined, whichever is less. It shows the apps in definition order.

When you select Throughput (Percentage of Actual Traffic) radio button, the chart displays the percentage of bytes sent and received since the app was defined. It shows the apps in definition order.

When you click on an application title on the left side of the chart (or right click in the chart), a dialog appears that displays the address for the application.

10.1.12 IP Addresses



IP Addresses displays the number of authorized IP Addresses in green and the numberof unauthorized IP Addresses in red.

Four buttons at the bottom of the page provide additional options for defining and viewing data.

Click on a row above to show addresses
Define Applications And Alarms
Define E-Mail Addresses
Define Authorized IP Addresses
Show IP Addresses Seen

Define Applications and Alarms

Define E-mail Addresses

Define Authorized IP Addresses

Show IP Addresses Seen

10.1.13 Dashboard - Define Applications and Alarms

The Applications and Alarms window is used to specify which ports are displayed in the Applications Distribution graph and the Network Alarms (Utilization) table.

1. On the Dashboard select the Define Applications and Alarms button.
2. Select Active App if you want the port to appear in the Applications Distribution graph.
3. Select Active Alarm if you want the port to appear in the Network Alarms (Utilization) table.
4. Enter a name for the port in the Application Name text box.
5. Enter the port number in the Port text box.
6. Select TCP, UDP, or Both from the combo box for the Port Type.
7. Enter a value for the low (Yellow) threshold for the Alarm Threshold (Utilization).

Note: The value of the Yellow threshold is the % of Max Utilization.

If the data equals or exceeds the Yellow threshold level, the Network Alarms (Utilization) table displays yellow and an e-mail is sent to each e-mail address specified in the Define E-Mail Addresses dialog. For example, if you set a Yellow threshold of 10% for HTTP and the activity equals or exceeds 10%, the background and circle next to HTTP turns yellow and e-mail is sent indicating a Yellow alarm condition.

8. 8. Enter a value for the high (Red) threshold for the Alarm Threshold (Utilization).

Note: The value of the Red threshold is the % of Max Utilization.

If the data equals or exceeds the Red threshold level, the Network Alarms (Utilization) table displays red and an e-mail is sent to each e-mail address specified in the Define E-Mail Addresses dialog. For example if you set a red threshold of 15% for HTTP and the activity equals or exceeds 15%, the background and the circle next to HTTP turns red and e-mail is sent indicating a Red alarm condition.

When the alarm clears (i.e. the data returns to a Green condition from either a Yellow or Red condition), the background and the appropriate circle turn green and e-mail is sent indicating that the alarm has cleared.

9. Enter a value (in seconds) for a minimum alarm condition duration.

This value identifies how long an alarm threshold must be equaled or exceeded before the alarm is indicated in the Network Alarms (Utilization) table and e-mail is sent. For example, let's say HTTP has a Yellow Alarm Threshold of 10%, with a Min Duration (secs) of 5. This means that the Alarm Threshold of 10% must be equaled or exceeded for at least five seconds for the alarm to show as yellow on the Network Alarms (Utilization) table and for e-mail to be sent.

10. Select Save.

If there are any errors in the settings a message is displayed listing each error. If there are no errors, the settings are saved.

10.1.14 Define Email Addresses

The **Define Email Addresses** window is used to enter email addresses that receive a message when an alarm condition is met or when an unauthorized IP address is detected on the NetDecoder Dashboard. There are two pieces of information you have to enter: mail server and email addresses.

1. On the Dashboard select the *Define Email Addresses*
2. Enter the *Mail Server* address.

To locate the Mail Server address in Outlook:

> Tools > Options > Mail Setup > E-mail Accounts > Data Files > Click on Mailbox - [Name] > Settings > General.

The **Microsoft Exchange server:** field contains the Mail Server address.

3. Enter one or more e-mail addresses

You can only have one email address per line. For multiple addresses, select Enter at the end of the line to move down.

4. Select *Send Test Message* to send a test message to the email addresses.

Once you verify that the mail server and email addresses have been entered correctly:

5. Select *Save.*

When a threshold is exceeded or an unauthorized IP address is seen, an email is sent to the email addresses.

10.1.15 Dashboard - Define Authorized IP Addresses

The Authorized IP Addresses window is used to specify which IP addresses are considered to be either authorized or unauthorized. These IP addresses are the source and destination addresses identified in packets during an analysis.

- Authorized IP addresses are specified in the top section. If this section is selected, all other IP addresses are considered unauthorized.
- Alternatively, unauthorized IP addresses can be specified in the bottom section. If this section is selected, only these IP addresses are considered unauthorized, and all other IP addresses are considered authorized.
- If an unauthorized IP address is detected, an e-mail warning is generated.

By default, all IP addresses are considered authorized.

A count of authorized and unauthorized IP addresses are indicated in the IP Addresses pie chart. The actual addresses are listed in the Show IP Addresses Seen dialog.

To enter an authorized IP address:

1. Select the Authorized IP Addresses radio button.
2. Enter an IP address by typing it in or by cutting and pasting from the Show IP Addresses Seen dialog.
3. Select Save

To enter an unauthorized IP address:

1. Select the Unauthorized IP Addresses radio button.
2. Enter an IP address by typing it in or by cutting and pasting from the Show IP Addresses Seen dialog.
3. Select Save

There are several items to remember when entering authorized or unauthorized IP addresses.

- You can enter one IP address per line.
- The last number in an IP address can be replaced by a dash-separated range (for example 192.168.0.10-20) or an asterisk (for example 192.169.0.*, which is equivalent to 192.169.0.0-255)
- E-mail is sent for the first occurrence of each IP address which is either in the unauthorized list or not in the authorized list (whichever list is selected).

10.1.16 Dashboard - Show IP Addresses Seen

The Authorized IP Addresses Seen window displays which IP addresses have been detected in packets. These packets can either be sent or received.

- Authorized IP addresses are shown in the top section.
- Unauthorized IP addresses are shown in the bottom section.

You specify whether an IP address is authorized or unauthorized using the Define Authorized IP Addresses dialog.

A count of authorized and unauthorized IP addresses detected are indicated in the IP Addresses pie chart. Authorized IP addresses detected are indicated in green. Unauthorized IP addresses detected are indicated in red.

Note: More than just a static display, you can copy and paste IP addresses from both the authorized and unauthorized sections of the dialog into the Define Authorized IP Addresses dialog.

11 Find

11.1 Starting a Search

You can search your data in several different ways. Some types of searches are relevant only for framed data and is not offered if the data is not framed. Other types of searches are available depending on the type of data being viewed.

To Begin a Search

1. Open a capture file, or capture some data to search.
2. Open the Event Display or Frame Display window.
3. Click on the *Find* icon or choose *Find* from the *Edit* menu.
4. The Find window has a tab for each type of search. Click on the appropriate tab for the type of search you want to do.
5. Select the parameters for your search, and click *Find Next*. *Find Next* looks for the next occurrence of the search criteria, while *Find Previous* looks for an earlier occurrence of the search criteria.
6. Press F3 to repeat the last search.

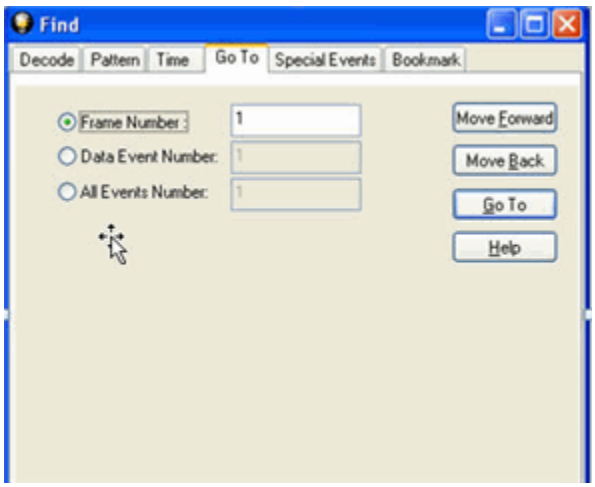
Search results are highlighted in the Event or Frame Displays, or both if appropriate. The selection in the Event Display appears on the third line down from the top of the window by default: this value can be changed.

11.2 Using Go To

This type of search allows you to go to a particular frame or event, or to move through the data X number of events or frames at a time. You can move either forward or backwards through the data.

To access the Go To function:

1. Select *Go To* from the *Edit* menu on the Frame Display, Event Display, or the Protocol Navigator. You can also click the Find icon on the toolbar
2. The system displays the Find dialog with the Go To tab selected.



Note: The tabs displayed on the Find dialog depend on the product you are running and the content of the capture file or buffer you are viewing.

To go to a particular frame :

1. Select the *Frame Number* radio button
2. Type the frame number in the box.
3. Click the *Go To* button.
4. To move forward or backward a set number of frames, type in the number of frames you want to move
5. Then click the *Move Forward* or *Move Back* button.

To go to a particular event :

1. Select the Data Event Number or All Events Number radio button.
2. Type the number of event in the box.
3. Click the Go To button.
4. To move forward or backwards through the data, type in the number of events that you want to move each time.
5. Then click on the Move Forward or Move Backward button.
6. For example, to move forward 10 events, type the number 10 in the box, and then click on Move Forward. Each time you click on Move Forward, FTS moves forward 10 events.

See Event Numbering for why the Data Event Number and All Events Number may be different. As a general rule, if you have the Show All Events icon depressed on the Event Display window or Frame Display Event pane, choose All Events Number. If the Show All Events button is up, choose Data Event Number.

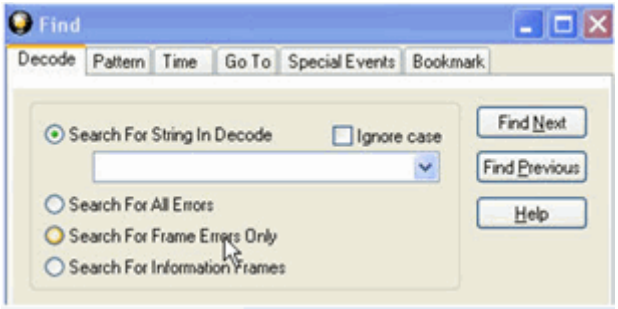
11.3 Searching for Frame Errors

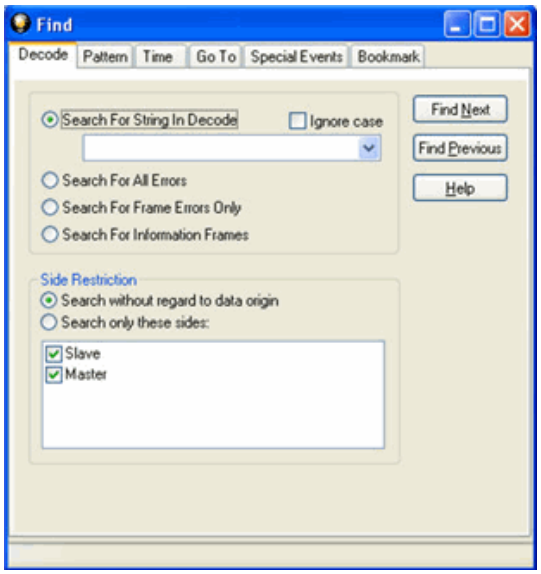
There are several options for error searching:

- Search for All Errors finds frame errors as well as frames with byte-level errors (such as parity or CRC errors).
- Search for Frame Errors Only finds Frame specific errors, such as Frame Check errors.
- Search for Information Frame only searches Information Frames

To access the search within decodes function:

1. Select *Find* from the *Edit* menu on the Frame Display, Event Display, or the Protocol Navigator. You may choose to select the Find icon from one of the toolbars
2. Click on the *Decode* tab of the Find dialog.
3. Click the appropriate radio button for the type of search you want to perform or enter a value
4. Click Find Next.





Note:

The tabs displayed on the Find dialog depend on the product you are running and the content of the capture file you are viewing.

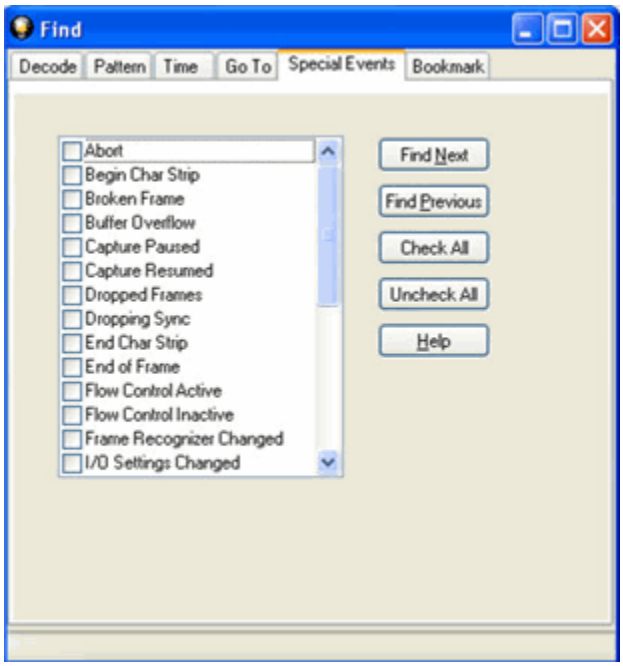
11.4Searching for Special Events

The analyzer inserts or marks events other than data bytes in the data stream.

For example, the analyzer inserts start-of-frame and end-of-frame markers into framed data, marking where each frame begins and ends. If a hardware error occurs, the analyzer shows this using a special event marker.

To access the search for special events function:

1. Select *Find* from the *Edit* menu on the Frame Display, Event Display, or the Protocol Navigator. You may choose to select the Find icon from one of the toolbars
2. Click on the *Special Events* tab of the Find dialog.



3. Check the event or events you want to look for in the list of special events.
4. Click Find Next.

Note:

The tabs displayed on the Find dialog depend on the product you are running and the content of the capture file you are viewing.

- Not all special events are relevant to all types of data. For example, control signal changes are relevant only to serial data and not to Ethernet data.

For a list of all special events and their meanings, see List of All Event Symbols.

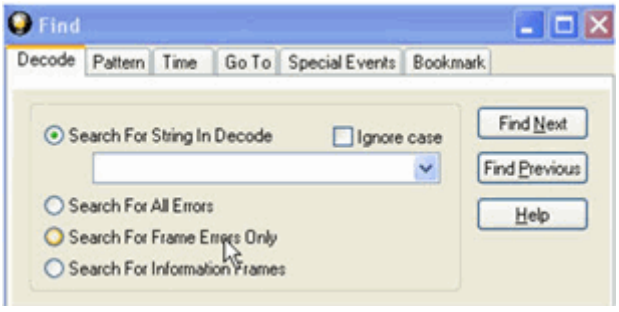
11.5 Searching within Decodes

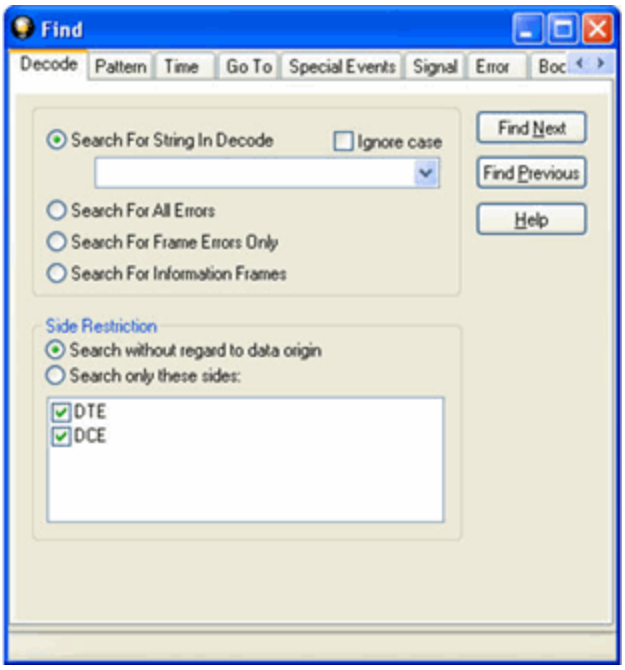
Searching within decodes lets you to do a string search on the data in the Decode Pane of the Frame Display window.

You can search one or both sides of the circuit, and your search can include wildcards. You can use characters, hex or binary digits, wildcards or a combination of any of the formats when entering your string.

To access the search within decodes function:

1. Select *Find* from the *Edit* menu on the Frame Display, Event Display, or the Protocol Navigator. You may choose to select the Find icon from one of the toolbars.
2. Click on the *Decode* tab of the Find dialog.





Note:

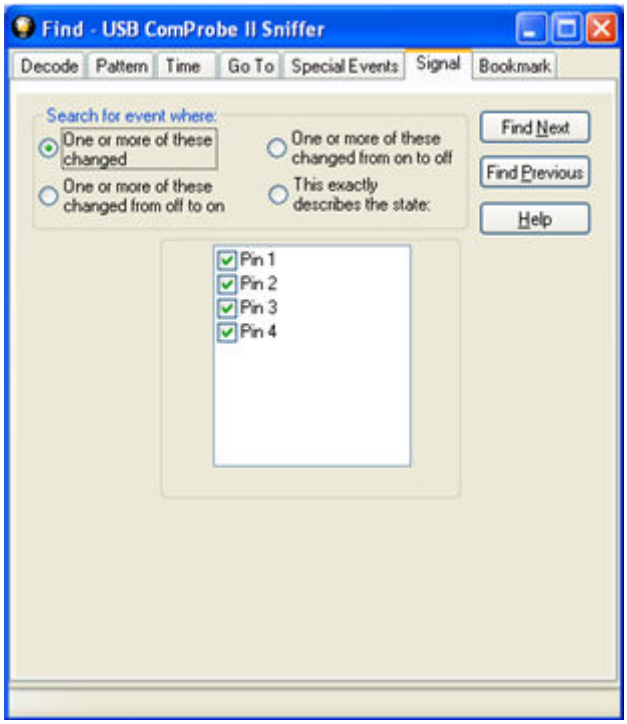
The tabs displayed on the Find dialog depend on the product you are running and the content of the capture file you are viewing.

11.6 Searching by Signal

You can search using information originating from the Breakout Box.

1. Select one or more of the *checkboxes* for Pin 1, 2, 3, or 4.
   Click here to learn more about the Breakout Box and Pins 1 - 4.

2. Select one of the *four radio buttons* to choose the condition that must be met in the search



3. Click *Find Next* to locate the next occurrence of the search criteria or *Find Previous* to locate an earlier occurrence of the search criteria.

11.7 Changing Where the Search Lands

When doing a search in the analyzer, the byte or bytes matching the search criteria are highlighted in the Event Display. The first selected byte appears on the third line of the display.

To change the line on which the first selected byte appears:

1. Open fts.ini (located in the C:\Program Files\Common Files\FTE)
2. Go to the [CVEventDisplay] section
3. Change the value for SelectionOffset.
4. If you want the selection to land on the top line of the display, change the SelectionOffset to 0 (zero).

11.8 Subtleties of Timestamp Searching

Timestamping can be turned on and off while data is being captured. As a result, the capture buffer may have some data with a timestamp, and some data without. When doing a search by timestamp, the analyzer ignores all data without a timestamp.

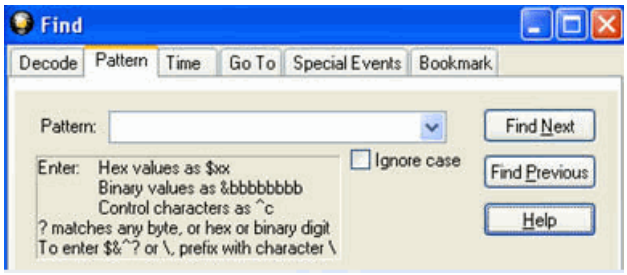
11.9 Entering Search Patterns (String Searches)

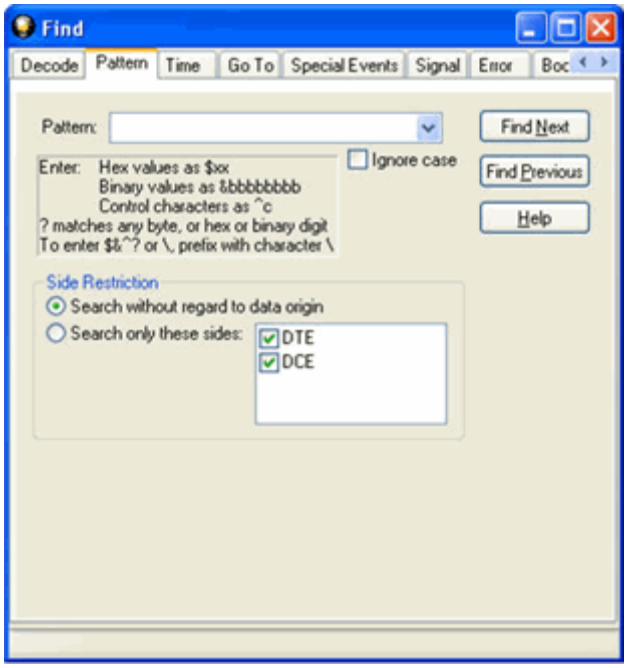
11.9.1 Searching by Pattern

Search by Pattern lets you perform a traditional string search. You can combine any of the formats when entering your string, and your search can include wildcards. You can search one or both sides of a circuit containing interwoven data such as serial communication.

To access the search by pattern function:

1. Select *Find* from the *Edit* menu on the Frame Display, Event Display, or the Protocol Navigator. You can also click the Find icon from one of the toolbars.
2. Click on the *Pattern* tab of the Find dialog.





Note:

The tabs displayed on the Find dialog depend on the product you are running and the content of the capture file you are viewing.

11.9.2 Entering Characters

Various characters are used when creating a search string on the Find dialog. You can enter any character from a character set, with the following exceptions: \$&^?. These characters are used as prefixes to let you to enter hex, binary, control or wildcard characters.

1. Place the cursor in the Pattern box and type in your string.
2. Click Find Next in order to find the next occurrence of the string.
3. Click on Find Next as many times as necessary until the analyzer has searched all the data.
4. Clicking on Find Previous searches the buffer backwards.

The escape character is the backslash \. Use this character when you want to search for one of the above restricted characters. For example, to search for a $, you enter \$. To search for a \, enter \\.

Check Ignore Case to do a case-insensitive search.

11.9.3 Entering Hex or Binary

Hex or Binary values are used when creating a search string on the Find dialog.

To enter a hex value :

1. Enter a $ followed by two hex digits.
2. For example, to search for hex 00 01, enter $00$01.
3. If you need to specify the $ as a character, use \$.
4. The $ symbol tells the analyzer that the following characters are hex digits

To enter a binary value:

- The & symbol tells the analyzer that a binary number comes next. For example, to search for binary 00001111, you would use &00001111.
- If you need to specify the & as a character, use \&.

11.9.4 Control Characters

Various control characters are used when creating a search string on the Find dialog. You can enter any character from a character set, with the following exceptions: \$&^?. These characters are unavailable. The ^ (caret) is used to enter the control characters Ctrl-A through Ctrl-Z and Ctrl-@,[,\,],- when using the ASCII character set. For example, ^A specifies Ctrl-A ($01) and ^@ specifies ASCII NUL ($00).

If you need to specify the ^ as a character, use \^.

Note that neither the ^ character nor control characters exist in Baudot, so attempts to search for the ^ character results in an error message. The ^ character exists in EBCDIC, but control characters do not. A search for ^A in EBCDIC matches any occurrence of ^A ($5F$C1). You do not need to use the escape character to search for a ^ character in EBCDIC.

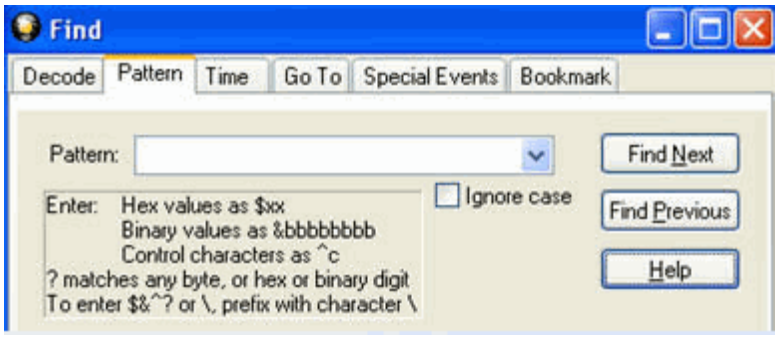
11.9.5 Wildcard Character

A wildcard can be used when creating a search string on the Find dialog.

The wildcard character is the question mark (?). The analyzer supports wildcard searching at the byte, nibble and bit level. Wildcards can be used in place of characters, hex digits, and binary digits. If you need to search for a ?, you can use \?.

11.9.6 Examples of Search Strings

In the Find function on the Frame Display, Event Display, or Protocol Navigator, you can search for any single byte in the range of hex $10 through $1F, type $1?.



&111111?? searches for binary numbers beginning with 111111 and ending with any combination of 1 and 0. 11111100, 11111101, 11111110, and 11111111 are all strings that match the search criteria.

To search for any four character string which starts with an L and ends with an ES, type L?ES.

You can combine formats in one string. For example, another way to specify a search for the string L?ES is $4C&????????&01000101S.

11.10 Searching by Time

11.10.1 Searching by Time

The analyzer can search by time in two different ways.

- **Absolute**

  An absolute timestamp search means that the analyzer searches for an event at the exact date and time specified. If no event is found at that time, the analyzer goes to the nearest event either before or after the selected time, based on the "Go to the timestamp" selection.

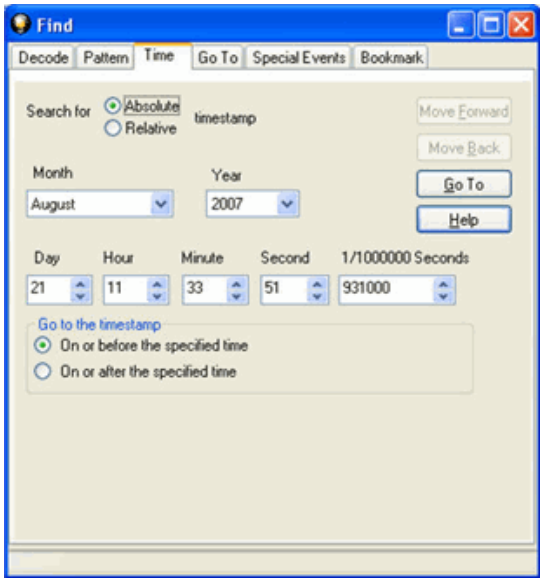
- **Relative**

  A relative search means that the analyzer begins searching from whatever event you are currently on, and search for the next event a specific amount of time away.

Note that the analyzer skips some special events that do not have timestamps, such as frame markers. Data events that do not have timestamps because timestamping was turned off either before or during capture are also skipped.

To access the search by time function:

1. Select *Find* from the *Edit* menu on the Frame Display, Event Display, or the Protocol Navigator. You may choose to select the Find icon from one of the toolbars.
2. Click on the *Time* tab of the Find dialog.
3. Use the "Search for" radio buttons at the top of the dialog to indicate the search type



Note:

The tabs displayed on the Find dialog depend on the product you are running and the content of the capture file you are viewing.

11.10.2 Searching with Absolute Timestamp

To access the search by time function:

1. Select *Find* from the *Edit* menu on the Frame Display, Event Display, or the Protocol Navigator. You may also select the Find icon from one of the toolbars
2. Click on the *Time* tab of the Find dialog.

Note: The tabs displayed on the Find dialog depend on the product you are running and the content of the capture file you are viewing.

3. Specify the time to search for by using the counters in the middle of the window.

   - Click on the arrows next to each item to increase or decrease the value of each counter.
   - By default, the counters display the timestamp of the first event in the file

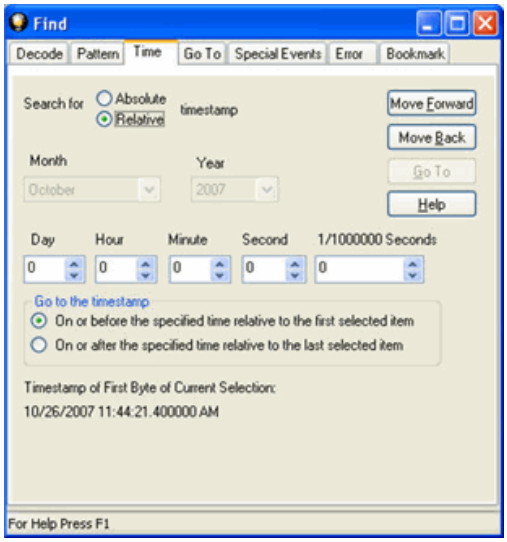
4. After selecting the time, click on the Go To button to start the search.

Sometimes there can be more than one event with the same timestamp. The system highlights all events with the specified timestamp.

11.10.3 Searching with Relative Timestamp

To access the search by time function:

1. Select *Find* from the *Edit* menu on the Frame Display, Event Display, or the Protocol Navigator. You can also select the Find icon from one of the toolbars.
2. Click on the *Time* tab of the Find dialog.



Note: The tabs displayed on the Find dialog depend on the product you are running and the content of the capture file or buffer you are viewing.

3. Click on the event in the Event Display window that you want to begin the search from. The event must have a timestamp in order for relative timestamp search to work.

4. In the *Find* dialog, use the counters in the middle of the window to specify the time interval you want to jump.
   You can specify intervals in days, hours, minutes, seconds, and fractions of a second, or any combination of these.

5. When you have specified the time interval you want to use, click on the Move Forward or Move Backward buttons to start the search from the current event.

For example, to search for an event occurring 10 seconds after the currently selected event, choose to do a relative timestamp search, use 10 seconds for your time interval, and click on Move Forward.

As with absolute timestamping, the analyzer highlights all events with the specified timestamp.

11.10.4 Choosing "On or Before" or "On or After"

The analyzer searches for an event that matches the time specified. If no event is found at the time specified, the analyzer goes to the nearest event either before or after the specified time. Choose whether to have the analyzer go to the nearest event before the specified time or after the specified time by clicking the appropriate radio button in the "Go to the timestamp" box.

If you are searching forward in the buffer, you usually want to choose the "On or After" button. If you choose the "On or Before" option, it may be that the analyzer finishes the search and not move from the current byte, if that byte happens to be the closest match.

12 Bookmarks

12.1 Bookmarks

- Bookmarks are a way to mark frames or events in a capture file. You can search for bookmarks and move quickly between bookmarks.
- Bookmarks appear as a magenta triangle next to the frame number in the Frame Display window. Any comment associated with the bookmark appears in the Bookmark column.
- When you add or change a bookmark, you are asked if you want to save your changes when you close the capture file, and given the option of saving the bookmarks to the current file or to a new one. See Confirming CFA Changes for more information.

12.2 Adding, Modifying or Deleting a Bookmark

You can Add, Modify, or Delete a Bookmark from the Add Bookmark dialog from the Frame Display, Event Display, or the Protocol Navigator.

Add:

1. Select the frame or event you want to bookmark.
2. Select *Add or Modify Bookmark* from the *Edit* menu on the Frame Display, Event Display, or the Protocol Navigator. Or simply select the *Add or Modify Bookmark* icon on one of the toolbars.
3. In the dialog box, add a comment if you wish.
4. Click *OK*.

You can also add a bookmark by right-clicking on the frame and choosing Add Bookmark from the right-click menu.

Modify and Delete:

1. Select the frame or event with the bookmark to be edited.
2. Select *Add or Modify Bookmark* from the *Edit* menu on the Frame Display , Event Display , or the Protocol Navigator . Or simply select the *Add or Modify Bookmark* icon on one of the toolbars.

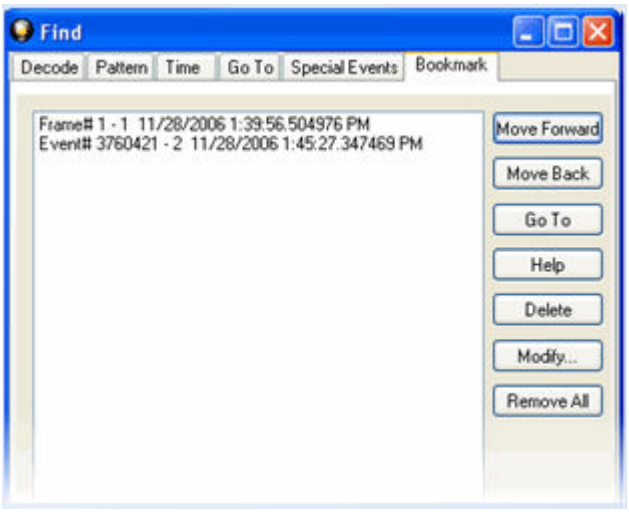
3. To modify a bookmark, change the comment in the dialog box and click OK.
4. To delete a bookmark, click the Delete button.

You can also modify or delete a bookmark by right-clicking on the frame and choosing Modify Bookmark from the right-click menu.

12.3 Displaying All and Moving Between Bookmarks

There are two ways to move between bookmarks.

1. Press the F2 key to move to the next frame or event with a bookmark.
2. Click the Display All Bookmarks icon . Select the bookmark you want to move to and click the Go To button, or simply double-click on the bookmark. Click the Move Forward and Move Back buttons to cycle through the bookmarks.



- To delete a bookmark, select it and click the Delete button.
- To modify a bookmark, select it and click the Modify button.
- Click Remove All to delete all the bookmarks.

13 Filtering

13.1 Difference Between Ethernet Capture Filters and Display Filters

There are two types of filters: Display filters and Ethernet capture filters.

An *Ethernet capture filter* looks at frames when they are first captured. If the frame satisfies the filter criteria, the frame is kept and put in the capture buffer. If the frame does not satisfy the filter criteria, it is thrown away. Data that is filtered out using an Ethernet capture filter cannot be recovered. Only one Ethernet capture filter can be active at a time. Capture filtering is not available in serial products yet.

A *display filter* looks at frames that have already been captured. It looks at every frame in the capture buffer and displays those that match the filter criteria. Frames that do not match the filter criteria are not displayed. Unlike an Ethernet capture filter, where data that does not match is thrown away, all the data is kept when using a display filter. The filter just displays a subset of the data. Multiple display filters can be used simultaneously, and different windows can be displaying data using different filters.

13.2 Display Filters

13.2.1 About Display Filters

Display filters allow a user to look at a subset of captured data without affecting the capture content. There are three general classes of display filters:

- Protocol Filters
- Named Filters
- Quick Filters

Protocol Filters

Protocol filters test for the existence of a specific single layer. The system creates a protocol filter for each decoder that is loaded if that layer is encountered in a capture session.

There are also three special purpose filters that are treated as protocol filters:

- All Frames with Errors
- All Frames with Bookmarks
- All Special Information Nodes

Named Filters

- Named filters test for anything other than simple single layer existence. Named filters can be constructed that test for the existence of multiple layers, field values in layers, frame sizes, etc., as well as combinations of those things. Named filters are persistent across sessions.
- Named filters are user-defined. User-defined filters persist in a template file. User defined filters can be deleted.

Quick Filters

- Quick Filters are combinations of Protocol Filters and/or Named Filters that are displayed on the Quick Filter tab.
- Quick Filters cannot be saved and do not persist across sessions.
- Quick Filters are created on the Quick Filter Dialog or through filter selection on the Protocol Navigator.

13.2.2 Including and Excluding Radio Buttons

All filter dialog boxes contain an "Include" and an "Exclude" radio button. These buttons are mutually exclusive. The "Include/Exclude" selection becomes part of the filter definition, and appears as part of the filter description displayed to the right of the Toolbar.

Include:

A filter constructed with the "Include" button selected, returns a data set that includes frames that meet the conditions defined by the filter and omits frames that do not.

Exclude:

A filter constructed with the "Exclude" button selected, returns a data set that excludes frames that meet the conditions defined by the filter and consists of frames that do not.

13.2.3 Creating a Display Filter

There are two steps to using a display filter. Define the filter conditions, and then apply the filter to the data set. The system combines both filter definition and application in one dialog.

1. Click the *Display Filters* icon on either the *Protocol Navigator* or the *Frame Display* window or select *Apply/Modify Display Filters* from the *Filter* menu to open the *Set Condition* dialog box.
2. Select Include or Exclude to
3. Select the initial condition for the filter from the drop-down list.
4. Set the parameters for the selected condition in the fields provided. The fields that appear in the dialog box are dependent upon the previous selection. Continue to enter the requested parameters in the fields provided until the condition statement is complete.

5. Click *OK*. The system displays the *Save Named Condition* dialog. Provide a name for the filter condition or accept the default name provided by the system and click OK. Prohibited characters are left bracket '[', right bracket ']' and equal sign '='. The *Set Condition* dialog box closes, creates a tab on the *Frame Display* with the filter name, and applies the filter.

The filter appears in the Quick Filtering and Hiding Protocols dialog also.

When a display filter is applied, a description of the filter appears to the right of the toolbar in both the *Protocol Navigator* and the *Frame Display* windows.

Notes:

The system requires naming and saving of all filters created by the user.

The *OK* button on the *Set Condition* dialog box is unavailable (grayed out) until the condition selections are complete.

When you have multiple Frame Display windows with a display filter or filters, those filter do not automatically appear in other Frame Display windows. You must use the Hide/Reveal feature to display a filter created in one Frame Display in different Frame Display window.

13.2.4 Named Display Filters

You can create a unique display filter by selecting a data type on the Frame Display and using a right click menu. When you create a Name Filter, it appears in the Quick Filtering dialog, where you can use it do customize the data you see in the Frame Display panes.

1. Select a frame in the Frame Display Summary Pane.
2. Right click in the one of the data columns in the Summary Pane: CRC, NESN, DS, Packet Success, Ethertype, Source Address, etc.
3. Select Filter in (data type)

The Filtering Results dialog appears.

4. Enter a name for the filter
5. Select OK.

The filter you just created appears in the Named Filters section of the Quick Filtering dialog.

13.2.5 Using Compound Display Filters

Compound filters use Boolean logic to create complex and precise filters. There are three primary Boolean logic operators: AND, OR, and NOT.

The AND operator narrows the filter, the OR operator broadens the filter, and the NOT operator excludes conditions from the filtered results. Include parentheses in a compound filter to nest condition sets within larger condition sets, and force the filter-processing order.

There are two steps to using a compound filter. Define the filter conditions, and then apply the filter to the data set. The analyzer combines both filter definition and application in one dialog.

1. Click the *Display Filters* icon on either the *Protocol Navigator* or the *Frame Display* window or select "Apply/Modify Display Filters" from the filter menu to open the *Set Condition* dialog box.
2. Click the *Advanced* button on the *Set Condition* dialog box.
3. Select the initial condition for the filter from the combo box.
4. Set the parameters for the selected condition in the fields provided. The fields that appear in the dialog box are dependent upon the previous selection. Continue to enter the requested parameters in the fields provided until the conditions statement is complete.
5. Click the Plus icon on the left side of the dialog box and repeat steps 3 and 4 for the next condition. Continue adding conditions until your filter is complete.
6. Include parentheses as needed and set the Boolean operators.
7. Click *OK*. The system displays the *Save Named Condition* dialog. Provide a name for the filter condition or accept the default name provided by the system and click *OK*. The *Set Condition* dialog box closes, creates a tab on the Frame Display with the filter name, and applies the filter.

When a display filter is applied, a description of the filter appears to the right of the toolbar in both the Protocol Navigator and the Frame Display windows.

Note:

Use the *Up* and *Down* arrow icons on the left side of the dialog box to order your conditions, and the *Delete* button to delete conditions from your filter.

The *OK* button on the *Set Condition* dialog box is unavailable (grayed out) until the condition selections are complete.

13.2.6 Defining Node and Conversation Filters

There are two steps to using Node and Conversation display filter. Define the filter conditions, and then apply the filter to the data set. The analyzer combines both filter definition and application in one dialog.

1. Click the *Display Filters* icon on either the *Protocol Navigator* or the *Frame Display* window or select "Apply/Modify Display Filters" from the filter menu to open the *Set Condition* dialog box.
2. Choose "frames with the conversation" as the initial condition from the *Select* combo box.
3. Select an address type from the *Type* combo box (The address type selection populates both Address combo boxes with node address in the data set that match the type selection).
4. Select a node address from the first *Address* combo box.
5. Choose a direction arrow from the *Direction* box. The left arrow filters on all frames where the top node address is the destination, the right arrow filters on all frames where the top node address is the source, and the double arrow filters on all frames where the top node address is either the source or the destination.
6. If you want to filter on just one node address, skip step 7 & 8, and continue with step 9.
7. If you want to filter on traffic going between two address nodes (i.e. a conversation), select an address type for the second node address from the *Type* combo box.
8. Select a node address from the second *Address* combo box.
9. Click *OK*. The *Set Condition* dialog box closes and the analyzer applies the filter.

When a display filter is applied, a description of the filter appears to the right of the toolbar in both the *Protocol Navigator* and the *Frame Display* windows.

Note:

The *OK* button is unavailable (grayed out) until the condition selections are complete.

13.2.7 Using Advanced Display Filtering Techniques

Intermediate to advanced users, with a solid knowledge of filter definition and application may find it useful to create some of the more common filters "on the fly" using the advanced filtering techniques.

Choose one of the panes in either the *Frame Display* or *Protocol Navigator* windows:

1. Place the cursor over a parameter you wish to filter on such as a node address or protocol type, and right click.
2. A pop up menu appears with selections for filtering.
3. Select the filter.

4. The system either closes the menu and applies the filter, or displays the *Set Conditions* dialog box with the known parameters filled in and the additional options available to complete the conditions statement.

13.2.8 Deleting and Hiding Display Filters

13.2.8.1 The Difference Between Deleting and Hiding Display Filters

If you wish to remove a filter from the system permanently, then use the Delete procedure. However, if all you want to do is remove a filter as a means to un-clutter the display, then use the Hide procedure.

Deleting a saved filter removes the filter from the current session and all subsequent sessions. In order to retrieve a deleted filter, the user must recreate it using the *Set Conditions* dialog.

Hiding a filter merely removes the filter from the display. A hidden filter can be reapplied using the Show/Hide procedure.

13.2.8.2 Deleting Saved Display Filters

1. Select *Delete Display Filters* from the *Filter* menu in either the *Protocol Navigator* or the *Frame Display* window to open the *Delete Named Condition* dialog. The system displays the *Delete Named Condition* dialog with a list of all user defined filters.
2. Select the filter to be deleted from the drop-down list.
3. Click the *Delete* button.
4. Click *OK*. The *Delete Named Condition* dialog box closes and the system deletes the filter.

13.2.8.3 Hiding/Revealing a Display Filter

1. Select "Hide/Show Display Filters" from the filter menu on either the *Protocol Navigator* or the *Frame Display* window to open the *Hide/Show* dialog. The system displays the *Hide/Show* dialog with a list of all user defined filters.
2. Select the filter to be hidden from the combo box.
3. Click the *Hide* button.
4. Click *OK*. The *Hide/Show* dialog box closes, and the system hides the filter and removes the filter tab from the *Frame Display*.

Revealing a Hidden Display Filter

There are several ways to reveal a hidden filter. One can open the *Quick Filter* dialog and check the box next to the hidden filter, or check the box next the hidden filter in the *Protocol Navigator* display.

Perform the following actions to reveal a hidden filter:

1. Select "Hide/Show Display Filters" from the filter menu in either the *Protocol Navigator* or the *Frame Display* window to open the *Hide/Show* dialog. The system displays the *Hide/Show* dialog with a list of all user defined filters.
2. Select the filter to be revealed from the combo box.
3. Click the *Show* button.
4. Click *OK*. The *Hide/Show* dialog box closes and the system reveals the filter and adds the filter tab to the *Frame Display*.

Note: When you have multiple Frame Display windows with a display filter or filters, those filter do not automatically appear in other Frame Display windows. You must use the Hide/Reveal feature to display a filter created in one Frame Display in different Frame Display window.

13.2.9 Editing Filters

13.2.9.1 Modifying a Condition in a Filter

1. Click the *Display Filters* icon on either the *Protocol Navigator* or the *Frame Display* window or select "Apply/Modify Display Filters" from the *Filter* menu to open the *Set Condition* dialog box. The *Set Condition* dialog box displays the current filter definition. To display another filter, click the *Open* icon, and select the filter from the Popup list of all the saved filters.
2. Edit the desired parameter of the condition.
   Because the required fields for a condition statement depend upon previously selected parameters, the Set Condition dialog box may display additional fields that were not present in the original filter. In the event this occurs, continue to enter the requested parameters in the fields provided until the condition statement is complete.
3. Click *OK*. The system displays the *Save Named Condition* dialog. Ensure that the filter name is displayed in the text box at the top of the dialog, and click *OK*. (If you choose to create an additional filter, then provide a new name for the filter condition or accept the default name provided by the system and click *OK*.) The *Set Condition* dialog box closes, and the system applies the modified filter.

Note:

When a display filter is applied, a description of the filter appears to the right of the toolbar in both the *Protocol Navigator* and the *Frame Display* windows.

The *OK* button on the *Set Condition* dialog box is unavailable (grayed out) until the condition selections are complete.

13.2.9.2 Deleting a Condition in a Filter

1. Click the *Display Filters* icon on either the *Protocol Navigator* or the *Frame Display* window or select "Apply/Modify Display Filters" from the *Filter* menu to open the *Set Condition* dialog box. The *Set Condition* dialog box displays the current filter definition. To display another filter, click the *Open* icon, and select the filter from the Popup list of all the saved filters.
2. Select the desired condition from the filter definition.
3. Click the Delete icon.
4. Edit the Boolean operators and parentheses as needed.
5. Click *OK*. The system displays the *Save Named Condition* dialog. Ensure that the filter name is displayed in the text box at the top of the dialog, and click *OK*. (If you choose to create an additional filter, then provide a new name for the filter condition or accept the default name provided by the system and click *OK*.) The *Set Condition* dialog box closes, and the system applies the modified filter.

Note:

When a display filter is applied, a description of the filter appears to the right of the toolbar in both the *Protocol Navigator* and the *Frame Display* windows.

The *OK* button on the *Set Condition* dialog box is unavailable (grayed out) until the condition selections are complete.

13.2.9.3 Renaming a Display Filter

1. Select "Rename Display Filters" from the *Filter* menu in either the *Protocol Navigator* or the *Frame Display* window to open the *Rename Filter* dialog. The system displays the *Rename Filter* dialog with a list of all user defined filters.
2. Select the filter to be renamed from the combo box.
3. Enter a new name for the filter in the text box.
4. Click *OK*. The *Rename Filter* dialog box closes and the system renames the filter.

13.3 Ethernet Capture Filters

13.3.1 Creating and Using an Ethernet Capture Filter

There are two steps to using an Ethernet capture filter. Define the filter conditions, and then apply the filter to the steaming data. FTS combines both filter definition and application in one dialog.

1. Select "I/O Settings" from the *Options* menu.
2. Click the *Define Conditions* tab.

3. FTS supports four different types of filters. Click on the links below for more information about defining each type of filter.
   BPF (Create a custom filter)
   Node (Includes filtering on a Ethernet single node as well as conversations between nodes)
   Pattern
   Predefined (Includes protocols and protocol specific filters)
4. After you define the filter, click the *Capture Filters* tab.
5. Choose the filter or filters to apply. See Applying An Ethernet Capture Filter.
6. Click *OK*. The filters dialog closes and FTS applies the filter.

Note:

Ethernet Capture filtering is not available when viewing a capture file. Ethernet Capture filters look at frames as they are being captured and either discards them or puts them in the buffer based on the filter criteria. Display filters look at the frames in the buffer and display only those frames that match the criteria.

13.3.2 Applying an Ethernet Capture Filter

Note:Ethernet Capture filters are unavailable when viewing a capture file.

1. Select "I/O Settings" from the *Options* menu to display the capture filter dialog.
2. Click on the *Capture Filters* tab at the top of the dialog.
3. In the tree view on the left, click the condition you want to apply, and then click the arrow buttons to move the condition to the *Conditions Selected in Filter* box. You may choose more than one condition to include in the filter.
4. The *Filter Representation* box at the bottom of the dialog displays text describing the filter. Click the checkbox to see the tcpdump syntax.
5. If you make a mistake and want to start over, click the Reset button.
6. [Optional] Type a name in the Compound Filters box at the top of the dialog and click the *Save Compound Filter* icon. In the future, you will be able to select the same condition(s) by selecting the name from the box.
7. Click *OK* (at the bottom of the far left side of the dialog). The filters dialog closes and FTS applies the capture filter.

When using an Ethernet capture filter, the *Control* window displays text describing the capture filter conditions to the right of the toolbar, and the *Control* window status bar displays "Run-Filter" as the "Capture Status".

Ethernet Capture filters look at data as it is being captured, and stores only those frames that match the filter criteria in the buffer.

13.3.3 Removing an Ethernet Capture Filter

Removing an Ethernet capture filter can be done by following the steps below :

1. To remove an Ethernet capture filter, select "I/O Settings" from the *Options* menu to display the filters dialog.
2. Click on the *Capture Filters* tab at the top of the dialog.
3. FTS displays the Ethernet capture filter currently in use in the *Conditions Selected in Filter* box. Click the condition(s) you want to remove. Use the arrow buttons to move the conditions to the box on the left, OR click the double arrow button to remove all conditions.
4. Click *OK* (at the bottom of the far left side of the dialog). The Filters dialog closes and FTS removes the filter.

13.3.4 Defining Node and Conversation Ethernet Capture Filters

1. Select "I/O Settings" from the *Options* menu.
2. Click on the *Define Conditions* tab at the top of the dialog.
3. In the tree view on the left, click the word *Node*. The right side of the dialog changes to display the Node definition pane.
4. If you want to include all frames matching your filter, select the *Include* radio button at the center top of the pane. If you want to exclude all frames matching your filter (and therefore see everything but those frames), click the *Exclude* radio button (See Including and Excluding Radio Buttons).
5. In the *Node A* section, select the radio button for the type of address you want. All means to pass all frames. Type the MAC or IP address of the node you wish to filter on.
6. Choose a direction arrow from the Direction box. The left arrow filters on all frames where Node A is the destination, the right arrow filters on all frames where Node A is the source, and the double arrow filters on all frames where Node A is either the source or the destination.
7. If you want to filter on just one node, stop right here. Click the *Add* button at the bottom of the pane to finish your filter and add it to the filter tree on the left side of the dialog.
8. If you want to filter on traffic going between two nodes (i.e. a conversation), select an address type and add the MAC or IP address of the second node in the Node B box. Click the *Add* button at the bottom of the pane to finish your filter and add it to the filter tree on the left side of the window.

Optional Filter Naming

Before clicking the *Add* button, type a name in the *Name* box after defining the filter, click *Add*, and the name appears in the left side of the dialog.

13.3.5 Selecting Predefined Ethernet Capture Filters

1. Select "I/O Settings" from the *Options* menu.
2. Click on the *Capture Filters* tab at the top of the dialog.
3. In the tree view on the left, click the plus sign next to the word Predefined to expand that section.
4. Click the condition you want to apply, and then click the arrow buttons to move the condition to the *Conditions Selected in Filter* box. You may choose more than one condition to include in the filter.
5. Click *OK*. The filter dialog closes and FTS applies the filter.

Predefined filters are not editable. FTS supplies many predefined filters applicable to the protocols available. This section shows the available predefined filters.

13.3.6 Defining Pattern or Offset Ethernet Capture Filters

1. Select "I/O Settings" from the *Options* menu.
2. Click on the *Define Conditions* tab at the top of the dialog.
3. In the tree view on the left, click the word *Pattern*. The right side of the dialog changes to display the Pattern definition pane.
4. If you want to include all frames matching your filter, select the *Include* radio button at the top of the pane. If you want to exclude all frames matching your filter (and therefore see everything but those frames), click the *Exclude* radio button (See Including and Excluding Radio Buttons).
5. Enter a pattern in the *Look for this Pattern* box. Use $ to specify a hex byte (e.g. $00 looks for a null character).
6. Enter the offset and where the offset should start in the *Offset this many bytes:* and *From start of:* boxes. FTS can begin counting from the start of the frame or the start of a protocol header. An offset of 0 means to look at the first byte, an offset of 1 means to look at the second byte, etc.
7. Click the *Add* button at the bottom of the pane to finish your filter and add it to the filter tree on the left side of the dialog.

Optional Filter Naming

Before clicking the *Add* button, type a name in the *Name* box after defining the filter, click *Add*, and the name appears in the left side of the dialog.

13.3.7 Using BPF to Create a Custom Ethernet Capture Filter

You can create, modify, and delete filters using the I/O menu items on the Protocol Navigator and Frame Display dialogs.

1. Select "I/O Settings" from the *Options* menu.
2. Click on the *Define Conditions* tab at the top of the dialog.

3. In the tree view on the left, click the word *BPF*. The right side of the dialog changes to display the BPF definition pane.
4. If you want to include all frames matching your filter, select the *Include* radio button at the top of the pane. If you want to exclude all frames matching your filter (and therefore see everything but those frames), click the *Exclude* radio button (See Including and Excluding Radio Buttons).
5. Enter the BPF string in the *Expression* box (See Berkeley Packet Filtering Man Page).
6. Click the *Add* button at the bottom of the pane to finish your filter and add it to the filter tree on the left side of the dialog.

Optional Filter Naming

Before clicking the *Add* button, type a name in the *Name* box after defining the filter, click *Add*, and the name appears in the left side of the dialog.

Filtering functionality is based on Berkeley Packet Filtering (BPF), which is implemented in the UNIX program tcpdump. The Filter String Formats help topic describes how to write a filter string for the most common types of filters. For the full description of BPF syntax, click here for the instructions from the tcpdump man page.

13.3.8 Creating/Deleting a Compound Filter

A compound filter is a set of conditions grouped together to create a more complex filter which can then be named as a separate filter.

It's a convenient way of grouping conditions into one filter set and remembering what the filter does. Compound filters can be selected from a list on the *Capture Filters* tab, making it very easy to reuse groups of conditions.

To create a compound filter:

1. Move the conditions to the Select Filters to Apply box
2. Click the Save Compound Filter button.
3. Give the filter a name.

To delete a compound filter:

1. Select the filter from the list box
2. Click the *Delete Filter* button. This deletes the filter only. It does not delete the conditions used in the filter.

Compound filters also appear in the Named Filters box on the Protocol Navigator window. This lets you quickly apply the filter from the Protocol Navigator without having to open the Filters dialog.

13.3.9 Naming Ethernet Capture Filters

You can name any condition to something more meaningful to you. For example, you can name Node filters of IP addresses to show the name of the device corresponding to that address.

To name a filter:

1. Select "I/O Settings" from the *Options* menu to display the filter dialog.
2. Click on the *Define Conditions* tab at the top of the dialog.
3. Define the filter in the BPF, Node or Pattern sections of the *Define Conditions* tab.
4. Add a name in the *Name* box.
5. When you click the *Add* button, the name displays in the tree in the left pane.

Named filters also appear in the *Named Filters* box on the Protocol Navigator window. This lets you quickly apply the filter from the *Protocol Navigator* without opening the filters window.

13.3.10 Modifying a Condition in an Ethernet Capture Filter

1. Select "I/O Settings" from the *Options* menu to display the filter dialog.
2. Click on the *Define Conditions* tab at the top of the dialog.
3. In the tree view on the left, click the condition you want to modify. The right side of the dialog changes to display the definition pane for the type of condition selected and places the contents of the condition in the pane.
4. Change the condition to the desired state.
5. Click the Modify button at the bottom of the definition pane, and click the *OK* button at the bottom of the dialog.

13.3.11 Deleting a Condition in an Ethernet Capture Filter

1. Select "I/O Settings" from the *Options* menu to display the filter dialog.
2. Click on the *Define Conditions* tab at the top of the dialog.
3. In the tree view on the left, click the condition you want to delete. The right side of the dialog changes to display the definition pane for the type of condition selected, and put the contents of the condition in the pane.
4. Click the *Delete* button at the bottom of the definition pane, and click the *OK* button at the bottom of the dialog.

13.3.12 Filter Formats

13.3.12.1 Filter String Formats

Filtering functionality in the analyzer is based on Berkeley Packet Filtering (BPF), which is implemented in the UNIX program tcpdump. Because BPF was designed to filter Ethernet data, there are some limitations when filtering other types of data. For the full description of BPF syntax, click here for an excerpt from the tcpdump man page.

The filter format consists of one or more "qualifiers", which may or may not be followed by an ID, which identifies the thing to be filtered on.

Qualifiers

There are three kinds of qualifiers: type, direction and protocol.

- *Type qualifiers* tell you what kind of thing the ID refers to. There are three possible types: host, net and port. If no type is given, host is assumed.
- *Direction qualifiers* specify the direction of traffic to or from the ID. There are four possible directions:
  - src - source. Filters on frames for which the ID is the source.
  - dst - destination. Filters on frames for which the ID is the destination.
  - src or dst - source or destination. Filters on frames for which the ID is either the source or the destination.
  - src and dst - source and destination. Filters on frames for which the ID is both the source and the destination

  If no direction is given, src or dst is assumed.
- *Protocol qualifiers* specify a particular protocol. Possible protocol qualifiers are: ether, fddi, ip, arp, rarp, decnet, lat, sca, moprc, mopdl, tcp and udp, where ether stands for Ethernet. If no protocol is given, all protocols consistent with the type are assumed.

IDs, or Identifiers

Identifiers are usually a name or a number identifying a particular node, protocol, network, etc. Examples are Ethernet MAC addresses or IP addresses. To specify a hex value, use 0x before the value. Example: 0x50.

Expressions and Relational Operators

You can combine identifiers using the following:

- 'and' or '&&' - concatenation. Filters on frames where both identifiers are true.
- 'or' or '||' - alternation. Filters on frames where one or both of the identifiers is true.
- 'not' or '!' - negation. Excludes a frame if the identifier is true.
- Negation has highest precedence and is evaluated first. Alternation and concatenation have equal precedence and are evaluated left to right.

- Use parentheses to combine expressions. Example: to filter on all frames from Abel and either Baker or Charlie, use: host Abel and (Baker or Charlie)

Filter on MAC Address

To filter on all frames to and from an Ethernet MAC Address, use the following syntax:

ether host 00:01:02:03:04:05

To filter on all frames to and from two MAC Addresses:

ether host 00:01:02:03:04:05 and 06:07:08:09:0a:0b

Filter on IP Address

To filter on all frames to and from an IP address, use the following syntax:

ip host 100.200.300.4

To filter on all frames to and from two IP addresses, use:

ip host 100.200.300.4 and 100.200.300.5

Filter on Protocol

To filter on a protocol, enter the protocol name in the string box. Possible protocols are: ether, fddi, ip, arp, rarp, decnet, lat, sca, moprc, mopdl, tcp and udp, where ether stands for Ethernet. You can also filter on protocols within protocols using the proto keyword.

Examples:

- ip - filters on all IP frames
- ip proto \tcp - filters on all TCP frames (tcp is a keyword and must be escaped using the '\' when used as an ID)
- port 80 - filters on all frames 'to and from' a TCP port, in this case port 80 (HTTP)

Filter at an Offset

To specify an offset from a protocol, place the value in brackets.

ether[13]>5 - examines the 13th byte from Ethernet start of frame for a value greater than 5 (remember that the first byte is at offset zero).

13.3.12.2 Berkeley Packet Filtering Main Page

The following text is taken from the tcpdump main page. References to CShell have been removed, along with some references to escape characters which are relevant only when running tcpdump under CShell and which are not relevant to filtering in FTS.

Expression selects which packets are dumped. If no *expression* is given, all packets on the net are dumped. Otherwise, only packets for which *expression* is `true' are be dumped. The *expression* consists of one or more *primitives*. Primitives usually consist of an *id* (name or number) preceded by one or more qualifiers. There are three different kinds of qualifier:

type qualifiers say what kind of thing the id name or number refers to. Possible types are **host**, **net** and **port**. E.g., `host foo', `net 128.3', `port 20'. If there is no type qualifier, **host** is assumed.

dir	qualifiers specify a particular transfer direction to and/or from id. Possible directions are **src**, **dst**, **src** or **dst** and **src** and **dst**. E.g., `src foo', `dst net 128.3', `**src** or **dst** port ftp-data'. If there is no dir qualifier, src or dst is assumed. For `null' link layers (i.e. point to point protocols such as slip) the **inbound** and **outbound** qualifiers can be used to specify a desired direction.
proto	qualifiers restrict the match to a particular protocol. Possible protos are: **ether, fddi, ip, arp, rarp, decnet, lat, sca, moprc, mopdl, tcp** and **udp**. E.g., `ether src foo', `arp net 128.3', `tcp port 21'. If there is no proto qualifier, all protocols consistent with the type are assumed. E.g., `src foo' means `(ip or arp or rarp) src foo' (except the latter is not legal syn- tax), `net bar' means `(ip or arp or rarp) net bar' and `port 53' means `(tcp or udp) port 53'. [`fddi' is actually an alias for `ether'; the parser treats them identically as meaning ``the data link level used on the specified network interface.'' FDDI headers contain Ethernet-like source and destination addresses, and often contain Ethernet-like packet types, so you can filter on these FDDI fields just as with the analogous Ethernet fields. FDDI headers also contain other fields, but you cannot name them explicitly in a filter expression.]

In addition to the above, there are some special `primitive' keywords that don't follow the pattern: **gateway, broadcast, less, greater** and **arithmetic** expressions. All of these are described below.

More complex filter expressions are built up by using the words **and**, **or** and **not** to combine primitives. E.g., `host foo and not port ftp and not port ftp-data'. To save typing, identical qualifier lists can be omitted. E.g., `tcp dst port ftp or ftp-data or domain' is exactly the same as `tcp dst port ftp or tcp dst port ftp-data or tcp dst port domain'. Allowable primitives are:

dst host *host*	True if the IP destination field of the packet is *host*, which may be either an address or a name.
src host *host*	True if the IP source field of the packet is *host*.
host *host*	True if either the IP source or destination of the packet is *host*. Any of the above host expressions can be prepended with the keywords, **ip**, **arp**, or **rarp** as in: **ip host** *host* which is equivalent to: **ether proto** *ip* and **host** *host* If *host* is a name with multiple IP addresses, each address is checked for a match.
ether dst *ehost*	True if the ethernet destination address is *ehost*. *Ehost* may be either a name from /etc/ethers or a number for numeric format.
ether src *ehost*	True if the ethernet source address is *ehost*.
ether host *ehost*	True if either the ethernet source or destination address is *ehost*.

gateway *host*	True if the packet used *host* as a gateway. I.e., the ethernet source or destination address was *host* but neither the IP source nor the IP destination was *host*. *Host* must be a name and must be found in both /etc/hosts and /etc/ethers. (An equivalent expression is **ether host** *ehost* and **not host** *host* which can be used with either names or numbers for *host* / *ehost*.)
dst net *net*	True if the IP destination address of the packet has a network number of *net*. *Net* may be either a name from /etc/networks or a network number for details).
src net *net*	True if the IP source address of the packet has a network number of *net*.
net *net*	True if either the IP source or destination address of the packet has a network number of *net*.
net *net* **mask** *mask*	True if the IP address matches *net* with the specific netmask. May be qualified with **src** or **dst**.
net *net/len*	True if the IP address matches *net* a netmask *len* bits wide. May be qualified with **src** or **dst**.
dst port *port*	True if the packet is ip/tcp or ip/udp and has a destination port value of *port*. The *port* can be a number or a name used in /etc/services. If a name is used, both the port number and protocol are checked. If a number or ambiguous name is used, only the port number is checked (e.g., **dst port 513** prints both tcp/login traffic and udp/who traffic, and **port domain** prints both tcp/domain and udp/domain traffic).
src port *port*	True if the packet has a source port value of *port*.
port *port*	True if either the source or destination port of the packet is *port*. Any of the above port expressions can be prepended with the keywords, **tcp** or **udp**, as in: **tcp src port** *port* which matches only tcp packets whose source port is *port*.
less *length*	True if the packet has a length less than or equal to *length*. This is equivalent to: **len <=** *length*.
greater *length*	True if the packet has a length greater than or equal to *length*. This is equivalent to: **len >=** *length*.
ip proto *protocol*	True if the packet is an ip packet of protocol type *protocol*. *Protocol* can be a number or one of the names *icmp*, *igrp*, *udp*, *nd*, or *tcp*. Note that the identifiers *tcp*, *udp*, and *icmp* are also keywords and must be escaped via backslash (\).
ether broadcast	True if the packet is an ethernet broadcast packet. The *ether* keyword is optional.
ip	True if the packet is an IP broadcast packet. It checks for both the all-

broadcast	zeroes and all-ones broadcast conventions, and looks up the local subnet mask.
ether multicast	True if the packet is an ethernet multicast packet. The *ether* keyword is optional. This is shorthand for `**ether[0] & 1 != 0**'.
ip multicast	True if the packet is an IP multicast packet.
ether proto *protocol*	True if the packet is of ether type *protocol*. *Protocol* can be a number or a name like *ip*, *arp*, or *rarp*. Note these identifiers are also keywords and must be escaped via backslash (\). [In the case of FDDI (e.g., `**fddi protocol arp**'), the protocol identification comes from the 802.2 Logical Link Control (LLC) header, which is usually layered on top of the FDDI header. *Tcpdump* assumes, when filtering on the protocol identifier, that all FDDI packets include an LLC header, and that the LLC header is in so-called SNAP format.]
decnet src *host*	True if the DECNET source address is *host*, which may be an address of the form ``10.123'', or a DECNET host name. [DECNET host name support is only available on Ultrix systems that are configured to run DECNET.]
decnet dst *host*	True if the DECNET destination address is *host*.
decnet host *host*	True if either the DECNET source or destination address is *host*.
ip, arp, rarp, decnet	Abbreviations for: **ether proto** *p* where *p* is one of the above protocols.
lat, moprc, mopdl	Abbreviations for: **ether proto** where *p* is one of the above protocols. Note that *tcpdump* does not currently know how to parse these protocols.
tcp, udp, icmp	Abbreviations for: **ip proto** *p* where *p* is one of the above protocols.
expr relop expr	True if the relation holds, where *relop* is one of >, <, >=, <=, =, !=, and *expr* is an arithmetic expression composed of integer constants (expressed in standard C syntax), the normal binary operators [+, -, *, /, &, |], a length operator, and special packet data accessors. To access data inside the packet, use the following syntax: *proto* [*expr* : *size*] *Proto* is one of **ether**, **fddi**, **ip**, **arp**, **rarp**, **tcp**, **udp**, or **icmp**, and indicates the protocol layer for the index operation. The byte offset, relative to the indicated protocol layer, is given by *expr*. *Size* is optional and indicates the number of bytes in the field of interest; it can be either one, two, or four, and defaults to one. The length operator, indicated by the keyword **len**, gives the length of the packet. For example, `**ether[0] & 1 != 0**' catches all multicast traffic. The expression `**ip[0] & 0xf != 5**' catches all IP packets with options. The

expression `**ip[6:2] & 0x1fff = 0**' catches only unfragmented datagrams and frag zero of fragmented datagrams. This check is implicitly applied to the **tcp** and **udp** index operations. For instance, **tcp[0]** always means the first byte of the TCP *header*, and never means the first byte of an intervening fragment. Primitives may be combined using a parenthesized group of primitives and operators.

Negation (`**!**' or `**not**').

Concatenation (`**&&**' or `**and**').

Alternation (`**||**' or `**or**').

Negation has highest precedence. Alternation and concatenation have equal precedence and associate left to right.

Note that explicit **and** tokens, not juxtaposition, are now required for concatenation. If an identifier is given without a keyword, the most recent keyword is assumed. For example, **not host vs and ace** is short for **not host vs and host ace** which should not be confused with **not (host vs or ace)**.

EXAMPLES

To print all packets arriving at or departing from sundown:

host sundown

To print traffic between helios and either hot or ace:

host helios and (hot or ace)

To print all IP packets between ace and any host except helios:

ip host ace and not helios

To print all traffic between local hosts and hosts at Berkeley:

net ucb-ether

To print all ftp traffic through internet gateway snup:

gateway snup and (port ftp or ftp-data)

To print traffic neither sourced from nor destined for local hosts (if you gateway to one other net, this stuff should never make it onto your local net).

ip and not net localnet

To print the start and end packets (the SYN and FIN packets) of each TCP conversation that involves a non-local host.

tcp[13] & 3 != 0 and not src and dst net localnet

To print IP packets longer than 576 bytes sent through gateway snup:

gateway snup and ip[2:2] > 576

To print IP broadcast or multicast packets that were not sent via ethernet broadcast or multicast:

ether[0] & 1 = 0 and ip[16] >= 224

To print all ICMP packets that are not echo requests/replies (i.e., not ping packets):

icmp[0] != 8 and icmp[0] != 0

AUTHORS

Van Jacobson, Craig Leres and Steven McCanne, all of the Lawrence Berkeley National Laboratory, University of California, Berkeley, CA. Full Copyright notice.

13.3.13 Saving and Loading Capture Filter Files

13.3.13.1 Saving Ethernet Capture Filters to a File

From the Frame Display or Protocol Navigator windows:

1. Select "I/O Settings" from the *Options* menu to display the filters dialog.
2. Click on the *Define Conditions* tab at the top of the window.
3. Define one or more conditions.
4. Enter a name for the filter in the *Name*: field.
5. Click OK.

Saving a filter file saves the conditions you've created. You can combine these conditions in multiple ways to create different Ethernet capture filters.

If you create a condition set (a group of conditions to apply all at the same time) for an Ethernet capture filter and want to save the condition set, name the filter, and then save the filter file. The named filter is saved as part of the filter file, and is available the next time the file is opened.

13.3.13.2 Opening an Ethernet Capture Filter File

From the Frame Display or Protocol Navigator windows:

1. Select "I/O Settings" from the *Options* menu to display the filters dialog.
2. Select *File >Open* icon and browse to the filter file.

Filter files have a .filter extension by default. The default location for filter files is the **My Configurations** directory. However, the user may choose to set another default location using the Changing Default File Locations procedure.

3. Open the file.

13.4 Protocol Filtering from the Frame Display

13.4.1 Easy Protocol Filtering

There are two types of easy protocol filtering. The first method lets you filter on the protocol shown in the *Summary* pane, and the second lets you filter on any protocol discovered on the network so far.

13.4.2 Filtering On the Summary Layer Protocol

To filter on the protocol in the *Summary* in the Frame Display window pane:

1. Select the tab of the desired protocol, or open the *Summary Layer* combo box.
2. Select the desired protocol.
3. To filter on a different layer, just select another tab, or change the layer selection in the combo box.

13.4.3 Quick Filtering on a Protocol Layer

1. To filter on any protocol layer, open either the *Frame Display* or *Protocol Navigator* window.
2. On the *Frame Display* window, click the starred *Quick Filtering* icon or select "Quick Filtering" from the *Filter* menu.

This opens a dialog that lists all the protocols discovered so far. The protocols displayed change depending on the data received.

The box on the left is **Protocols To Filter In**.

- When you select the checkbox for a protocol in the **Protocols to Filter In**, the Summary Pane will only display those frames that contain data from that protocol.

If you filter on more than one protocol, the result are all frames that contain at least one of those protocols. For example, if you filter on IP and IPX NetBIOS, you receive all frames that contain either IP or IPX NetBIOS (or both). A Quick Filter tab then appears on the Frame Display labeled Quick Filter. Changing the filter definition on the Quick Filter dialog changes the filter applied on the Quick Filter tab. Quick filters are persistent during the session, but are discarded when the session is closed.

The box in the center is the **Protocols To Hide**.

- When you select the checkbox for a protocol in the **Protocols To Hide**, data for that protocol will not appear in the Decode, Binary, Radix, and Character Panes. The

frames containing that type data will still appear in the Summary Pane, but not in the Decode, Binary, Radix, and Character Panes.

The box on the right is the **Named Filters**. It contains filters that you create using the Named Filter and Set Condition dialogs.

- When you select the checkbox for the Name Filters, a tab appears on the Summary Pane that displays the frame containing the specific data identified in the filter. The named Filter tab remains on the Frame Display Summary Pane unless you hide it using the Hide/Show Display Filters dialog.

With **FBLEA**, the Configured BT Low energy devices and Exclude NULLSs and POLLs are default named filters.

3. Check the small box next to the name of each protocol you want to filter in, hide, or Named Filter to display.
4. Then click *OK*.

13.4.4 Filtering on all Frames with Errors from the Frame Display

To filter on all frames with errors:

1. Open the *Frame Display* window.
2. Click the starred *Quick Filter* icon or select "Quick Filtering" from the *Filter* menu
3. Check the box for *All Frames With Errors* in the "Protocols to filter in" pane, and click *OK.*
4. The system creates a tab on the *Frame Display* labeled *Quick Filter* that displays the results of the *All Frames With Errors* filter.

13.5 Protocol Filtering from the Protocol Navigator

13.5.1 Filtering on a Protocol Layer

You can filter on one or more protocol layers. The filter is inclusive which means only frames matching the filter you select are shown in the window. Frames that do not contain the protocol do not appear. You can filter on one protocol or several.

On the left side of the Protocol Navigator window are three panes. The top pane is the Frames Filtered In pane. In the pane is a list of all the protocols seen so far on the circuit.

1. Check the boxes next to the names of the protocols you want to filter in.

The data on the right side of the screen matches the filtering selected.

Three additional filters available are:

- All Frames With Bookmarks - filters in all frames with a *bookmark* associated with them.
- All Frames With Errors - filters in all frames with errors.
- All Special Information Nodes - filters in all *special information nodes* .

13.5.2 Filtering on all Frames with Bookmarks

To filter on all frames with bookmarks:

1. Open the *Protocol Navigator* window.
2. Check the *All Frames With Bookmarks* box in the top pane on the left side of the window.
3. To remove the filter, un-check the box.

13.5.3 Filtering on all Frames with Errors from the Protocol Navigator

To filter on all frames with errors :

1. Open the *Protocol Navigator* window.
2. Check the *All Frames With Errors* box in the top pane on the left side of the window.
3. To remove the filter, un-check the box.

13.5.4 Filtering on all Frames with Special Information Nodes

To filter on all frames with special information nodes:

1. Open the Protocol Navigator window.
2. Check the All Special Information Nodes box in the top pane on the left side of the window.
3. To remove the filter, un-check the box.

13.5.5 Named Filters

You can create, modify, and delete filters using the Filter menu items on the Protocol Navigator and Frame Display dialogs.

If you create a *Named* filter using the *Filters* dialog, the filter appears in the *Named Frame Filters* pane in the bottom left corner of the *Protocol Navigator* window.

1. Check the boxes next to the names of the filters you want to use.

Note that using a named filter affects the contents of the *Frame Display* window as well.

14 Saving Data

14.1 Saving Your Data

You can save all or part of a capture file. You can also load a previously saved capture file, and save a portion of that file to another file. This feature is useful if someone else needs to see only a portion of the data in your capture file.

On the Control toolbar you can set up to capture a single file or series of files. Click here to see those settings.

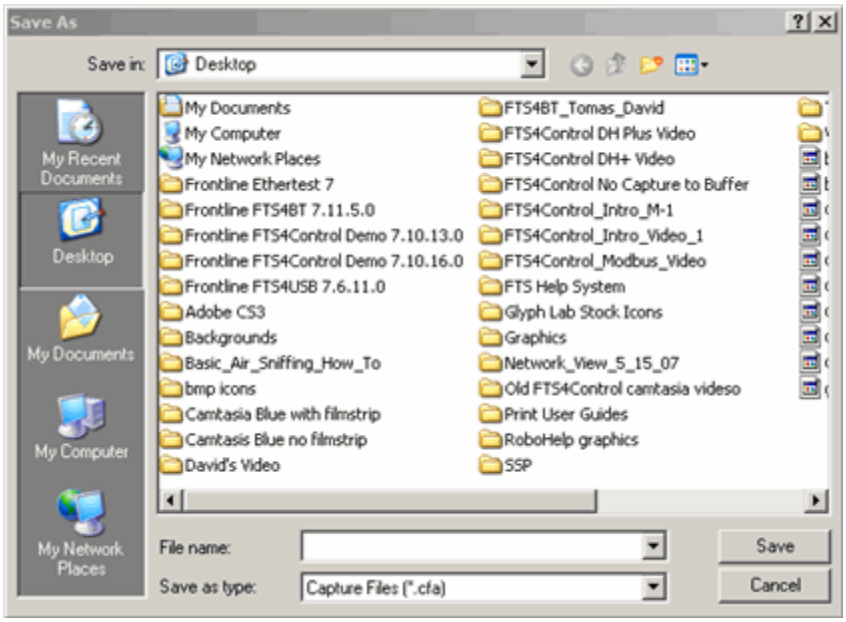
There are two ways to save portions or all of the data collected during a data capture. Click here to see how to capture data.

14.2 Saving the Entire Capture File using File > Save or the Save icon

This option is only available when you select Single File from the Capture Mode on System Settings. Click here to learn more about selecting Save options from System Settings.

1. If you are capturing data, click on the *Stop* icon to stop data capture. You cannot save data to file while it is being captured.
2. Open the *Event Display* or *Frame Display* window.

3. Click the *Save* icon, or select *Save* from the *File* menu.

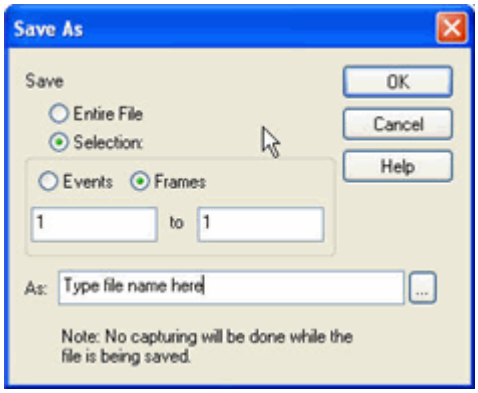


4. Type a filename in the *File name* box at the bottom of the screen.
5. Browse to select a specific directory. Otherwise your file is saved in the default capture file directory.
6. When you are finished, click *OK*.

14.3 Saving the Entire Capture File with Save Selection

1. If you are capturing data, click on the *Stop* icon to stop data capture. You cannot save data to file while it is being captured.
2. Open the *Event Display* or *Frame Display* window.
3. Right click in the data

4. Select *Save Selection* or *Save As* from the right click menu

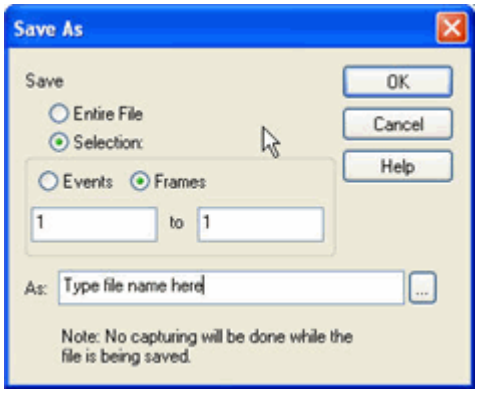


1. Click on the radio button labeled *Entire File*.
2. Choose to save *Events* or *Frames.* Choosing to save *Events* saves the entire contents of the capture file. Choosing to save *Frames* does not save all events in the capture file.
3. Type a filename in the *Save As* box at the bottom of the screen. Click the *Browse* icon to browse to a specific directory. Otherwise your file is saved in the default capture file directory.
4. When you are finished, click *OK*.

14.4 Saving a Portion of a Capture File

1. If you are capturing data, click on the *Stop* icon to pause data capture. You cannot save data to a file while it is being captured.
2. Open the *Event Display* or *Frame Display* window , depending on whether you want to specify a range in bytes or in frames.
3. Select the portion of the data that you want to save. Click and drag to select data, or click on the first item, move to the last item and Shift+Click to select the entire range, or use the Shift key with the keyboard arrows or the navigation icons in the Frame Display toolbar. If the range you want to save is too large to select, note the numbers of the first and last item in the range.
4. Right click in the data

5. Select *Save Selection* or *Save As* from the right click menu



6. Click on the radio button labeled *Selection*. If you selected a range, make sure the starting and ending numbers are correct. To specify a range, type the numbers of the first and last items in the range in the boxes.
7. Select either *Events* or *Frames* to indicate whether the numbers are event or frame numbers.
8. Type a filename in the *Save As* box at the bottom of the screen. Click the *Browse* icon to browse to a specific directory. Otherwise your file is saved in the default capture file directory.
9. Click *OK* when you are finished.

14.5 Confirm Capture File (CFA) Changes

This dialog appears when you close a capture file after changing the Notes, the protocol stack, or bookmarks. The dialog lists information that was added or changed and allows you to select which information to save, and whether to save it to the current file or to a new one.

Changes made to the file appear in a list in the left pane. You can click on each item to see details in the right pane about what was changed for each item. You simply check the boxes next to the changes you want to keep. Once you decide what changes to keep, select one of the following:

- Save To This File – Saves the changes you have made to the current capture file.
- Save As – Saves the changes to a new file.
- Cancel the Close Operation – Closes the file and returns you back to the display. No changes are saved.
- Discard Changes – Closes the file without saving any of the changes made to the notes, bookmarks, or protocol stack.

14.6 Adding Comments to a Capture File

The *Notes* feature allows you to add comments to a CFA file. These comments can be used for many purposes. For example, you can list the setup used to create the capture file, record why the file is useful to keep, or include notes to another person detailing which frames to look at and why. (Bookmarks are another useful way to record information about individual frames.)

To open the Notes window :

1. Click the Show Notes icon . This icon is present on the toolbars of the *Frame Display* , the *Protocol Navigator* , as well as the *Event Display* . *Notes* can be selected from the *Edit* menu on one of these windows.
2. Type your comments in the large edit box on the Notes window. The Cut, Copy, Paste, Undo and Redo features are all supported.
3. Click the thumbtack icon to keep the Notes window on top of any other windows.
4. When you're done adding comments, close the window.
5. When you close the capture file, you are asked to confirm the changes to the capture file. See Confirming Capture File (CFA) Changes for more information.

15 Loading and Importing Capture Files

15.1 Loading a Capture File

From the Control Window:

1. Go to the File menu.
2. Choose a file from the recently used file list.
3. If the file is not in the File menu list, select *Open Capture File* from the File menu or simply click on the *Open* icon on the Toolbar.
4. Capture files have a .cfa extension. Browse if necessary to find your capture file.
5. Click on your file, and then click Open.

15.2 Importing Capture Files

1. From the Control Window , go to the File menu and select *Open Capture File* or click on the *Open* icon on the Toolbar.
2. Change the Files of Type box to All Importable File Types or All Supported File Types. Select the file and click Open.

The analyzer automatically converts the file to the analyzer's format while keeping the original file in its original format. You can save the file in the analyzer's format, close the file without saving it in the analyzer's format, or have the analyzer automatically save the file in the analyzer's format (see the System Settings to set this option). All of these options keep your original file untouched.

When you first open the file, the analyzer brings up the Protocol Stack window and ask you what protocol decodes, if any, you want to use. You must choose a protocol decode at this point for the analyzer to decode the data in the file. If you open a file without using any decodes, and decide later that you want to apply a decode, choose Reframe from the File menu on the Control window.

At present, the analyzer supports the following file types:

- **Frontline Serialtest* Async and Serialtest ComProbe® for DOS** – requires the .byt for data and the .tim for timestamps (see note on importing DOS timestamps).
- **Greenleaf ViewComm* 3.0 for DOS** - requires the .byt for data and the .tim for timestamps (see note on importing DOS timestamps).
- **Frontline Ethertest* for DOS** – requires 3 files: filename.cap, filename.ca0 and filename.ca1.

- **Sniffer Type 1** – supports files with the .enc extension. Does not support Sniffer files with a .cap extension.
- **Snoop or Sun Snoop** – files with a .cap extension based on RFC 1761. For file format, see http://www.faqs.org/rfcs/rfc1761.html.
- **Shomiti Surveyor files in Snoop format** – files with a .cap extension. For file format, contact Technical Support.
- **CATC Merlin** - files with a .csv extension. Files must be exported with a specific format. See File Format for Merlin Files for information.
- **CATC Chief** - files with a .txt extension.

15.3 Converting Timestamps

Serialtest for DOS uses a timebase of Pacific Standard Time during non daylight savings time hours and Pacific Daylight Time during daylight savings time hours. The analyzer always uses Greenwich Mean Time (also known as Universal Time Coordinates).

When importing a Serialtest for DOS file, the analyzer must determine if the file was recorded during daylight savings time or not before converting the timestamps. Because the rules for determining this can change, it is possible for the analyzer to convert the timestamps incorrectly, resulting in timestamps that are off by one hour.

15.4 Adding Comments to a Capture File

The *Notes* feature allows you to add comments to a CFA file. These comments can be used for many purposes. For example, you can list the setup used to create the capture file, record why the file is useful to keep, or include notes to another person detailing which frames to look at and why. (Bookmarks are another useful way to record information about individual frames.)

To open the Notes window :

1. Click the Show Notes icon . This icon is present on the toolbars of the *Frame Display* , the *Protocol Navigator* , as well as the *Event Display* . *Notes* can be selected from the *Edit* menu on one of these windows.
2. Type your comments in the large edit box on the Notes window. The Cut, Copy, Paste, Undo and Redo features are all supported.
3. Click the thumbtack icon to keep the Notes window on top of any other windows.
4. When you're done adding comments, close the window.
5. When you close the capture file, you are asked to confirm the changes to the capture file. See Confirming Capture File (CFA) Changes for more information.

15.5 File Format for Merlin Files

FTS imports Merlin's export files that have been exported with Merlin's default settings. These files should have an extension of ".csv".

It is possible with the Merlin software to hide or change a field's format. If you do this before exporting the Merlin file then FTS may have trouble importing the file.

If you are experiencing problems importing Merlin files, then check to make sure that no fields were hidden and that the default field formats were being used, when the file was exported from Merlin.

16 Printing

16.1 Printing from the Frame Display/HTML Export

The Frame Display Print dialog and the Frame Display HTML Export are very similar. This topic discusses both dialogs.

The **Frame Display Print** dialog is directly below. The **Frame Display HTML Export** is located midway in this discussion.

About Frame Display Print

The Frame Display Print feature provides the user with the option to print the entire capture buffer or the current selection. When *Print Preview* is selected, the output displays in a browser print preview window, where the user can select from the standard print options. The output file format is in html, and uses the Microsoft Web Browser Control print options for background colors and images (see below).

Print Background Colors Using Internet Explorer

1. Open the Tools menu on the browser menu bar
2. Select "Internet Options…" menu entry.
3. Click Advanced tab.
4. Check "Print background colors and images" under the Printing section
5. Click the Apply button, then click OK

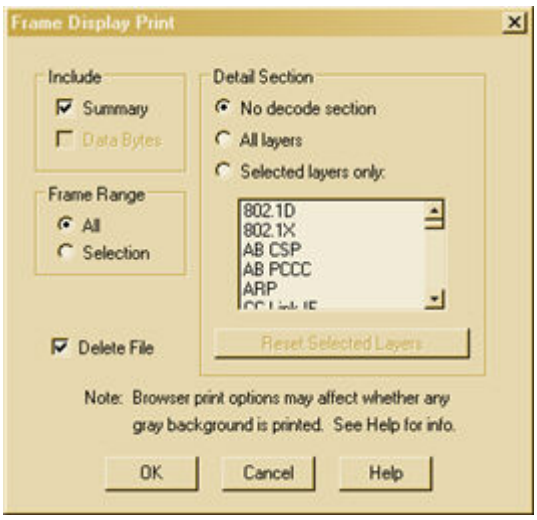
Configure the Print File Range in the Frame Display Print Dialog

Selecting more than one frame in the Frame Display window defaults the radio button in the Frame Display Print dialog to *Selection* and allows the user to choose the *All* radio button. When only one frame is selected, the *All* radio button in the Frame Display Print dialog is selected.

How to Print Frame Display Data

1. Select *Print* or *Print Preview* from the *File* menu on the Frame Display window to display the Frame Display Print dialog. Select *Print* if you just want to print your data to your default printer. Select *Print Preview* if you want access to printer options.
2. Choose to include the Summary Pane (check the box) in the print output. The summary Pane appears at the beginning of the printed output in tabular format. If you select All layers in the Detail Section, the **Data Bytes** option becomes available.
3. In the Detail Section, choose to exclude the decode from the Detail Pane in the Frame Display, or include All Layers or Selected Layers Only. If you choose to include selected layers, then select (click on and highlight) the layers from the list box. Click on selected layers in the list to de-select, or click the *Reset* button to de-select all selected layers.

CAUTION: Decode layers printout expanded regardless of the state of the Detail Pane in the Frame Display at the time of the request to print. This can produce a print output consisting of hundreds of pages or more. We recommend that you use *Print Preview* to determine the number of pages in your print output prior to printing.



Select the range of frames to include All or Selection in the Frame Range section of the Frame Display Print dialog.

Choosing *All* prints all of the frames in the capture file or buffer. If more than 1000 frames in the Frame Range, All will be disabled. You can still select more than 1000 frames using the Selection option, but when printing more than 1000 frames, there is the possibility that Print will not work properly.

Choosing *Selection* prints only the frames you select in the Frame Display window.

Note: Selecting the **Delete File** deletes the temporary html file that was used during printing..

4. Click the OK button.

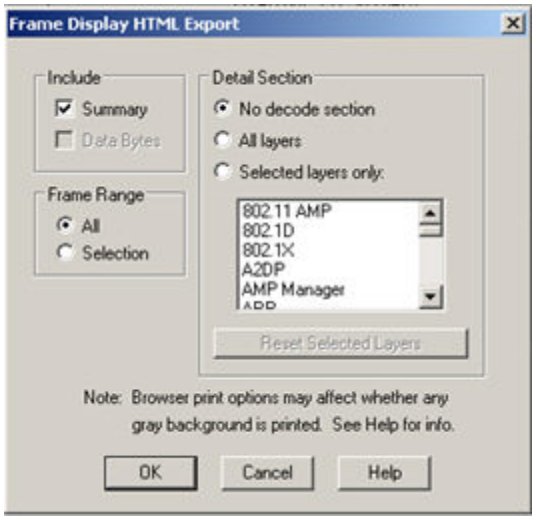
If you chose *Print Preview*, the system displays your data in a browser print preview display with options for printing such as page orientation and paper size. You can also use your Printer Preferences dialog to make some of these selections. When printing your data, the analyzer creates an html file and prints the path to the file at the bottom of the page. This file can be opened in your browser, however, it may appear different than the printed version.

16.2 Frame Display HTML Export

The Frame Display **HTML Export** feature provides the user with the option to export the entire capture buffer to an .html file.

How to export display data to an .html file

1. Select *HTML Export* from the *File* menu on the Frame Display window to display the **Frame Display HTML Export**.



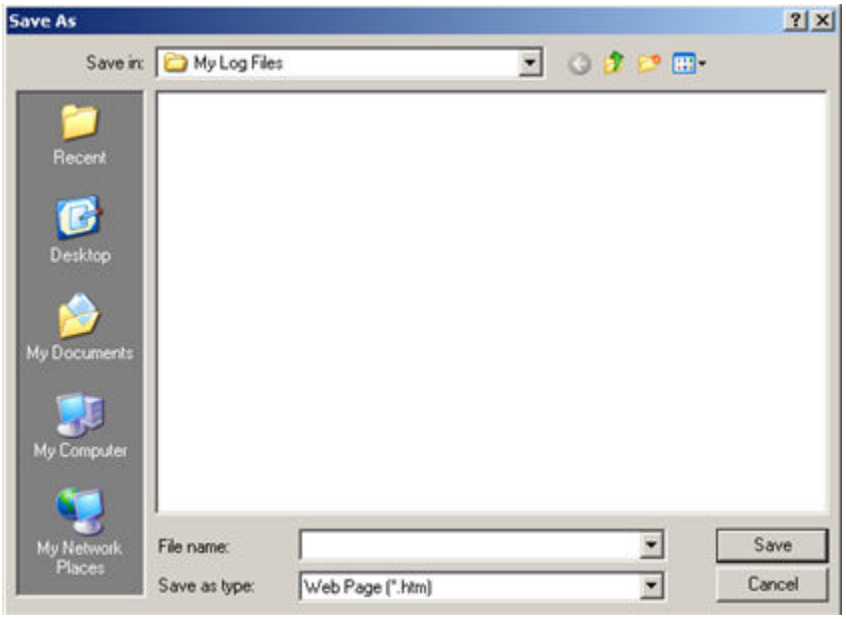
2. Choose to include the Summary Pane (check the box) in the .html output. If you select All layers in the Detail Section, the **Data Bytes** option becomes available.
3. In the Detail Section, choose to exclude the decode from the Detail Pane in the Frame Display, or include All Layers or Selected Layers Only. If you choose to include selected layers, then select (click on and highlight) the layers from the list box. Click on selected layers in the list to de-select, or click the *Reset* button to de-select all selected layers.
4. Select the range of frames to include *All* or *Selection* in the Frame Range section of the dialog.

   Choosing *Selection* includes only the frames you select in the Frame Display window.

Note: If the file size is too big, the Frame Range, **All**, will not be available. It will be grayed out.

5. Click the OK button.

The *Save As* dialog appears.



6. Enter a name for the file you want to save.

Note: There is no need to choose a file type. The file is saved as a .htm.

7. Select Save

The file is saved as a .htm file in the file location you chose.

16.3 Printing from the Event Display

About Event Display Print

The Event Display Print feature provides the user with the option to print either the entire capture buffer or the current selection. When *Print Preview* is selected, the output displays in a browser print preview window where the user can select from the standard print options. The output file format is in html, and uses the Microsoft Web Browser Control print options for background colors and images (see below).

Print Background Colors Using Internet Explorer

1. Open the Tools menu on the browser menu bar
2. Select "Internet Options…" menu entry.
3. Click Advanced tab.
4. Check "Print background colors and images" under the Printing section
5. Click the Apply button, then click OK

The Event Display Print feature uses the current format of the Event Display as specified by the user.

Note: See About Event Display for an explanation on formatting the Event Display prior to initiating the print feature.

Configure the Print File Range in the Event Display Print Dialog

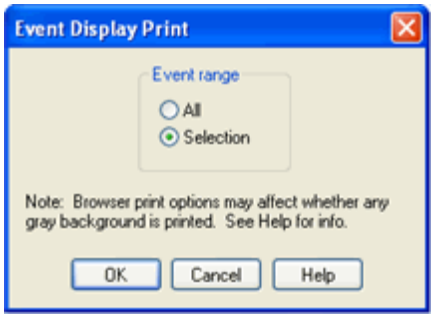
Selecting more than one event in the Event Display window defaults the radio button in the Event Display Print dialog to Selection and allows the user to choose the All radio button. When only one event is selected (can't have None selected), the *All* radio button in the Event Display Print dialog is selected.

How to Print Event Display Data to a Browser

1. Select *Print* or *Print Preview* from the *File* menu on the Event Display window to display the Event Display Print dialog. Select *Print* if you just want to print your data to your default printer. Select *Print Preview* if you want access to printer options.
2. Select the range of events to include from either *All* or *Selection* in the Event Range section of the Event Display Print dialog. Choosing *All* prints all of the events in the capture file or buffer. Choosing *Selection* prints only the selected events in the Event Display window.

   Note: In order to prevent a Print crash, you cannot select* All *if there are more than 100,000 events in the capture buffer.

Note: See Configure the Print File Range in the Event Display Print Dialog above for an explanation of these selections



3. Click the OK button.

If you chose *Print Preview*, the system displays your data in a browser print preview display with options for printing such as page orientation and paper size. You can also use your Printer Preferences dialog to make some of these selections. When printing your data, the analyzer creates an html file and prints the path to the file at the bottom of the page. This file can be opened in your browser, however, it may appear different than the printed version.

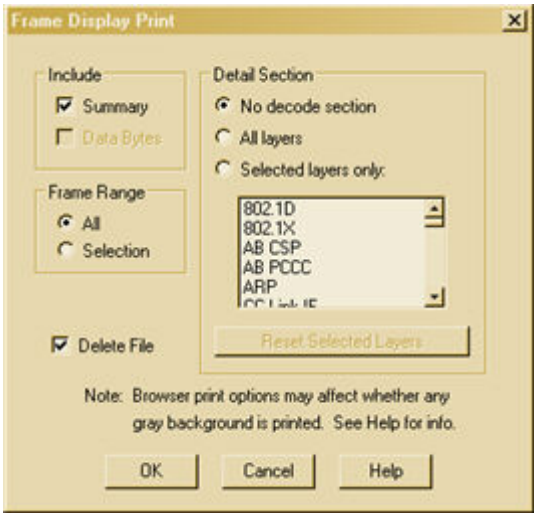
16.4 Print Preview

Print Preview gives a preview of how the data looks printed. You can scroll through the pages and zoom in on the data to get a closer look. The line of buttons across the top of the window controls the functions of the window.

To open the Print Preview window:

1. Choose Print Preview from the File menu in any window that supports printing.
2. Choose to include the Summary Pane (check the box) in the print output. The summary Pane appears at the beginning of the printed output in tabular format. If you select All layers in the Detail Section, the **Data Bytes** option becomes available.
3. In the Detail Section, choose to exclude the decode from the Detail Pane in the Frame Display, or include All Layers or Selected Layers Only. If you choose to include selected layers, then select (click on and highlight) the layers from the list box. Click on selected layers in the list to de-select, or click the *Reset* button to de-select all selected layers.

CAUTION: Decode layers printout expanded regardless of the state of the Detail Pane in the Frame Display at the time of the request to print. This can produce a print output consisting of hundreds of pages or more. We recommend that you use *Print Preview* to determine the number of pages in your print output prior to printing.



4. Select the range of frames to include All or Selection in the Frame Range section of the Frame Display Print dialog.

   Choosing *All* prints all of the frames in the capture file or buffer. If there are more than 1000 frames in the capture file or buffer, **All** will not be available.

   Choosing *Selection* prints only the selected frames in the Frame Display window.

Note: See Configure the Print File Range in the Frame Display Print Dialog above for an explanation of these selections.

Note: Selecting the **Delete File** deletes the temporary html file that was used during printing..

5. Click the OK button.

You can print directly from the Print Preview window.

- Next Page shows you how the next page in your data looks
- Prev Page takes you back to the previous page.
- Two Page changes the display to show two pages of data. When in the Two Page display, the button reads One Page. Click on the One Page button to return to viewing one page.
- Zoom In and Zoom Out allow you to change the magnification of the pages. Click on Zoom In to increase the magnification, and on Zoom Out to decrease the magnification. When you have reached the limit in either direction, the buttons is grayed out.
- You can also zoom in and out by clicking on the page itself. When the cursor looks like a magnifying glass, you can click on the page to increase the magnification. When you have reached the top level of magnification, the cursor changes back to an arrow. Click on the page to return to normal magnification.
- Click on the Close button to return to the regular display.

17 Exporting

17.1 Export

You can dump the contents of the Summary pane on the Frame Display into a Comma Separated File (CSV).

To access this feature:

1. Right click on the Summary Pane
2. Select the Export menu item
3. Enter a file name
4. Select Save

Another option to access quick export is :

1. Click on the File menu
2. Choose Export
3. Enter a file name
4. Select Save

17.2 Export Filter Out

You can filter out data you don't want or need in your text file.

(This option is available only for serial data.) In the Filter Out box, choose which side to filter out: the DTE data, the DCE data or neither side (don't filter any data.) For example, if you choose the radio button for DTE data, the DTE data would be filtered out of your export file and the file would contain only the DCE data.

You can also filter out Special Events (which is everything that is not a data byte, such as control signal changes and Set I/O events), Non-printable characters or both. If you choose to filter out Special Events, your export file would contain only the data bytes. Filtering out the non-printable characters means that your export file would contain only special events and data bytes classified as printable. In ASCII, printable characters are those with hex values between $20 and $7e.

17.3 Exporting Event Display to a File

About Event Display Export

The Event Display Export feature provides the following options:

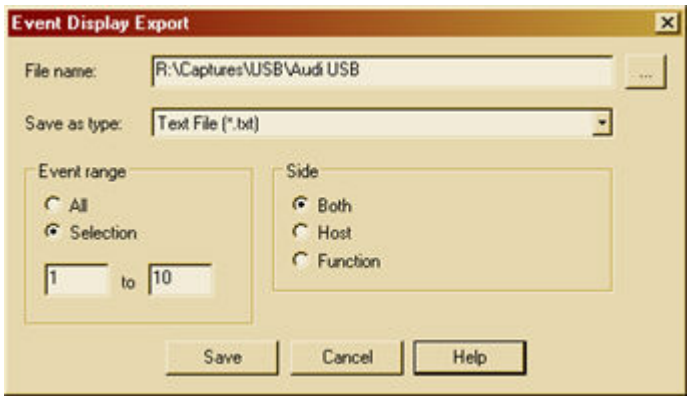
- Export either the entire capture buffer or the current selection
- Output file format as text, CSV, html, or bin.

The Event Display Export feature uses the current format of the Event Display as specified by the user.

Note: See About Event Display for an explanation on formatting the Event Display prior to initiating the export feature.

Accessing the Event Display Export Dialog

Selecting Export Events… from the File menu in the Event Display brings up the following dialog:



Configure the Export File Range in the Event Display Export Dialog

- Selecting more than one event in the Event Display window defaults the radio button in the Event Display Export dialog to Selection and allows the user to choose the All radio button.
- When only one event is selected (something must be selected), the All radio button in the Event Display Export dialog is selected by default.
- Side is used to determine whether you want to export data from a DCE/DTE, Slave/Master, Host/Function device or both.

How to Export Event Display Data to a File

1. Select Export Events… from the File menu on the Event Display window to display the Event Display Export dialog.

2. Enter a file path and name, or click the browser button to display the Windows Save As dialog and navigate to the desired storage location.
3. Select a file type from the Save as type: drop-down List Menu on the Event Display Export dialog.
4. Select from among the following file formats:

   Text File (*.txt)

   CSV File (*.csv)

   HTML File (*.html)

Binary File (*.bin)

5. Select the range of events to include in the file from either All or Selection in the Event Range section of the Event Display Export dialog.
   Note: See Configure the Export File Range in the Event Display Export Dialog above for an explanation of these selections.
6. Select a Side, either Host, Function, or Both
7. Click Save.

17.4 Exporting Baudot

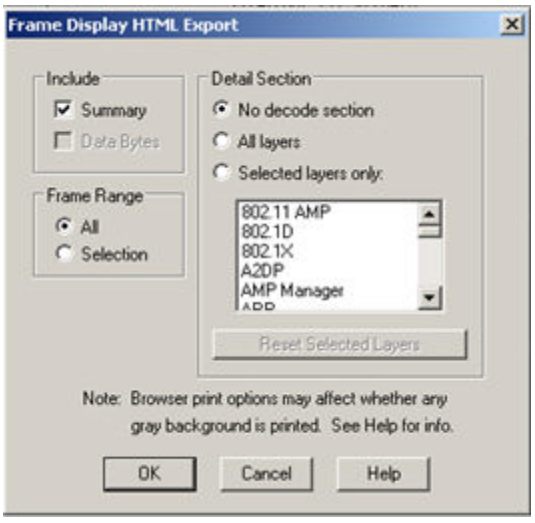
When exporting Baudot, you need to be able to determine the state of the shift character. In a text export, the state of the shift bit can be determined by the data in the Character field. When letters is active, the character field shows letters and vice versa.

17.5 HTML Export

The Frame Display **HTML Export** feature provides the user with the option to export the entire capture buffer to an .html file.

How to export display data to an .html file

1. Select *HTML Export* from the *File* menu on the Frame Display window to display the **Frame Display HTML Export**.



2. Choose to include the Summary Pane (check the box) in the .html output. If you select All layers in the Detail Section, the Data Bytes option becomes available.
3. In the Detail Section, choose to exclude the decode from the Detail Pane in the Frame Display, or include All Layers or Selected Layers Only. If you choose to include selected layers, then select (click on and highlight) the layers from the list box. Click on selected layers in the list to de-select, or click the Reset button to de-select all selected layers.

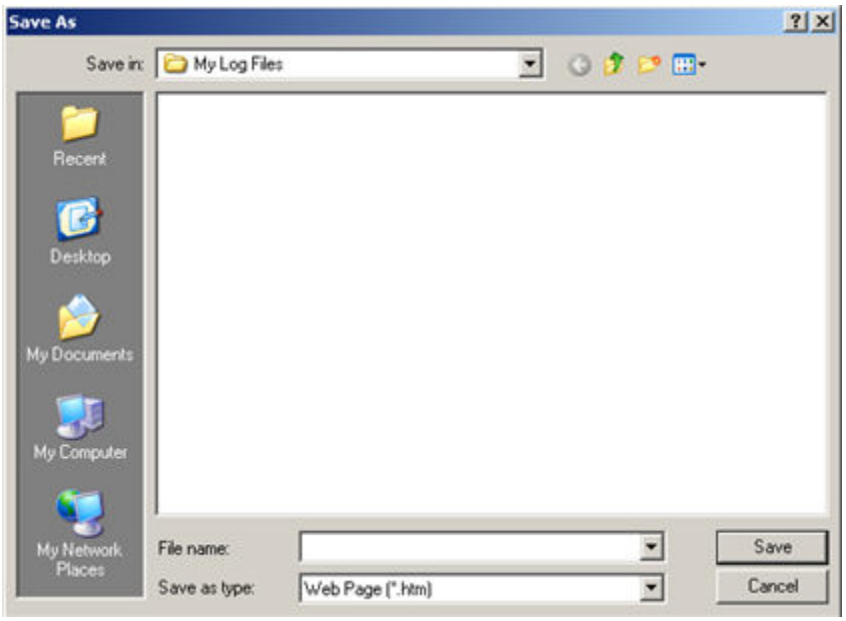
4. Select the range of frames to include All or Selection in the Frame Range section of the dialog.

   Choosing *Selection* includes only the frames you select in the Frame Display window.

Note: If the file size is too big, the Frame Range, **All**, will not be available. It will be grayed out.

5. Click the OK button.

The *Save As* dialog appears.



6. Enter a name for the file you want to save.

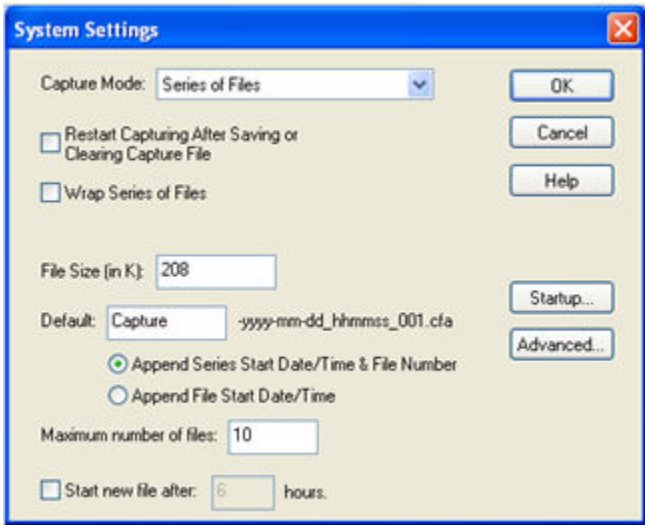
Note: There is not need to choose a file type. The file is saved as a .htm.

7. Select Save

18 System Settings and Program Options

18.1 System Settings

Open the System Settings window by choosing System Settings from the Options menu on the Control window. To enable a setting, click in the box next to the setting to place a checkmark in the box. To disable a setting, click in the box to remove the checkmark. When viewing a capture file, settings related to data capture are grayed out.



Capture Mode

- **Series of files**

  This option lets you capture to a series of files. The size of each file is no larger than the number given in File Size (in K),which has a maximum limit of approximately 176,000KB (1.7 GB) or 1/2 of the available hard disk space, whichever is **smaller**. The name of each file is the name you give it in the Name box followed by the date, time and a number. The date and time are when the series was opened. The number increments with each file. This guarantees unique file names are created.

  Set the maximum number of files in the series in the **Maximum number of files** box. The next file starts when the currently open file is full. If you want to start a new file on a periodic basis, check the box for **Start new file after** and put in the number of hours after which a new file is started. Note that if the currently open file becomes full before the time limit has been reached, a new file is opened immediately rather than lose data.

  Capturing stops if the maximum number of files has been used unless Wrap Files has been checked. If Wrap Files has been checked the analyzer erases the oldest file in the series and make a new file.

- **Single File**

This option allows the analyzer to capture data to a file without prompting you for a file name each time. The size of each file is not larger than the number given in File Size (in K). The name of each file is the name you give it in the Name box followed by the date and time. The date and time are when the series was opened.

Common Options

- **Restart Capturing After Saving or Clearing Capture File**

  If the Automatically Restart feature is enabled, the analyzer restarts capture to the file immediately after the file is closed.

- **Wrap File**

  When enabled, the analyzer wraps the file when it becomes full. The oldest events are moved out of the file to make room for new events. Any events moved out of the file are lost. When disabled, the analyzer stops capture when the file becomes full. Either reset the file or close your capture file to continue.

- **File Size (in K)**

  Enter the maximum size of the capture file, which is 176,000 KB, or 1/2 of the available hard drive space, whichever is **smaller**. If you enter a number larger than the maximum allowable size, the analyzer will display the allowable size.

- **Default**
  Enter a name for the capture file in the Default text box. Each saved file will begin with this name.

- **Append Series Start/Date & File Number**
  Select this radio button to automatically append a start date (yyyy-mm-dd_hhmmss) and file number (001) when capturing a series of files.

- **Append File Start Date/Time**
  Select this radio button to automatically append a start date (yyyy-mm-dd_hhmmss) when capturing a single file.

- **Start up**

  Opens the Program Start up Options window. Start up options let you choose whether to start data capture immediately on opening the analyzer.

- Advanced

  Opens the Advanced System Options window. The Advanced Settings should only be changed on advice of technical support.

18.2 System Settings - Disabled/Enabled Options

Some of the **System Settings** options are disabled depending upon the status of the data capture session.

- As the default, all the options on the System Settings dialog are enabled.
- Once the user begins to capture data by selecting the Start Capture button, some of the options on the System Settings dialog are disabled until the user stops data capture and either saves or erases the captured data.
- The user can go into the Startup Options and Advanced System Options on the System Settings dialog and make changes to the settings at any time.

18.3 Advanced System Options

These parameters affect fundamental aspects of the software, and it is unlikely that you ever have to change them. If you do change them and need to return them to their original values, the default value is listed in parentheses to the right of the value box.

Most technical support problems are not related to these parameters, and as changing them could have serious consequences for the performance of the analyzer, we strongly recommend contacting technical support before changing any of these parameters.

To access the Advanced System Options:

1. Go to the Control window.
2. Choose *System Settings* from the *Options* menu.
3. On the System Settings window, click the *Advanced* button.

- **Driver Receive Buffer Size in Kbytes**

  This is the size of the buffer used by the driver to store incoming data. This value is expressed in Kbytes.

- **Driver Action Queue Size In Operating System Pages**

  This is the size of the buffer used by the driver to store data to be transmitted. This value is expressed in operating system pages.

- **Frame Completion Timeout in Seconds**

  This is the number of seconds that the analyzer waits to receive data on a side while in the midst of receiving a frame on that side.

  If no data comes in on that side for longer than the specified number of seconds, an "aborted frame" event is added to the Event Display and the analyzer resumes decoding incoming data. This can occur when capturing interwoven data (DTE and DCE) and one side stops transmitting in the middle of a frame.

Aborted frames (just like broken frames and regular frames) are decoded and displayed in the Frame Display. If you experience aborted frames and suspect that your framed data may have pauses in it that exceed the specified timeout time, then you may want to increase that value.

The range for this value is from 0 to 999,999 seconds. Setting it to zero disables the timeout feature.

Note: This option is disabled when capturing data over Ethernet networks.

18.4 Changing Default File Locations

The analyzer saves user files in specific locations by default. Capture files are placed in the My Capture Files directory and configurations are put in My Configurations. These locations are set at installation.

Follow the steps below to change the default locations.

1. Choose Directories from the Options menu on the Control window to open the File Locations window.
2. Select the default location you wish to change.
3. Click Modify.
4. Browse to a new location.
5. Click OK.
6. Click OK when finished.

Note: If a user sets the **My Decoders** directory such that it is up-directory from an installation path, multiple instances of a personality entry may be detected, which causes a failure when trying to launch FTS. For example, if an FTS product is installed at **C:\FTS Stuff\My Products\Frontline FTS4BT w.x.y.z**, then "My Decoders" cannot be set to any of the following:

- C:\
- C:\FTS Stuff
- C:\FTS Stuff\My Products
- C:\FTS Stuff\My Products\Frontline FTS4BT w.x.y.z
- C:\FTS Stuff\My Products\Frontline FTS4BT w.x.y.z\App Data
- C:\FTS Stuff\My Products\Frontline FTS4BT w.x.y.z\App Data\Decoders
- or to any directory that already exists under C:\FTS Stuff\My Products\Frontline FTS4BT w.x.y.z\App Data\Decoders

Default Capture File Folder Checkbox

If the "Use Last Opened Folder for Capture Files" checkbox is checked, then the system automatically changes the default location for saving capture files each time you open a file from or save a file to a new location. For example, let's say the **default** location for saving capture files is **Drive A > Folder A**. Now you select the "Use Last Opened Folder for Capture Files" checkbox. The next time, however, you open a capture file from a different location, **Folder B > Removable Flash Drive**. Now when you save the capture file, it will be saved to **Folder B > Removable Flash Drive**. Also, all subsequent files will be saved to that location. This remains true until you open a file from or save a file to a different location.

There is one caveat to this scenario, however. Let's say you have selected "Use Last Opened Folder for Capture Files" and opened a file from a location other than the default directory. All subsequent capture files will be saved to that location. Suppose, however, the next time you want to save a capture file, the new file location is not available because the directory structure has changed: a folder has been moved, a drive has been reassigned, a flash drive has been disconnected, etc. In the case of a "lost" directory structure, subsequent capture files will be saved to the default location. FTS will always try to save a file to the folder where the last file was opened from or saved to, if "Use Last Opened Folder for Capture Files" is checked. If, however, the location is not accessible, files are saved to the default directory that is set at installation.

If the checkbox is unchecked, then the system always defaults to the directory listed in the File Locations dialog.

18.5 Selecting Start Up Options

1. To open this window:
2. Choose *System Settings* from the *Options* menu on the Control window.
3. On the System Settings window, click the *Start Up* button.
4. Choose one of the options to determine if the analyzer starts data capture immediately on starting up or not.

Don't start capturing immediately.

This is the default setting. The analyzer begins monitoring data but does not begin capturing data until the *Start Capture* icon on the Control, Event Display or Frame Display windows is clicked.

Start capturing to a file immediately.

When the analyzer starts up, it immediately opens a capture file and begin data capture to it. This is the equivalent of clicking the *Start Capture* icon. The file is given a name based on the settings for capturing to a file or series of files in the System Settings window.

Start capturing immediately to the following file:

Enter a filename in the box below this option. When the analyzer starts up, it immediately begins data capture to that file. If the file already exists, the data in it is overwritten.

Use this capture filter:

The drop down box lists all named filters. Select one that you want to use immediately on start up.

18.6 Timestamping

18.6.1 Timestamping Options

The Timestamping Options window allows you to enable or disable timestamping, and change the resolution of the timestamps for both capture and display purposes.

To open this window:

1. Choose *System Settings* from the *Options* menu on the Control window.
2. Click the *Set Timestamp Format* button.

OR

1. Click the Timestamping Options icon from either the Event Display or Statistics window.

OR

1. Click the Timestamping Options icon from the Event Display window.

18.6.2 Enabling/Disabling Timestamping

1. Choose *System Settings* from the *Options* menu on the Control window, and click the *Timestamping Options* button, or click the click the Timestamping Options icon from either the Event Display or Statistics window.
2. Check the *Store Timestamps* box to enable timestamping. Remove the check to disable timestamping. If you disable timestamping, you are not able to do delta or rate calculations.

18.6.3 Switching Between Relative and Absolute Time

With Timestamping you can choose to employ Relative Time or Absolute time.

1. Choose *System Settings* from the *Options* menu on the Control window, and click the *Timestamping Options* button, or click the click the Timestamping Options icon from either the Event Display or Statistics window.

2. Go to the *Display Options* section at the bottom of the window and find the *Display Relative Timestamps* checkbox.
3. Check the box to switch the display to relative timestamps. Remove the check to return to absolute timestamps.

Note: The options in this section affect only how the timestamps are displayed on the screen, not how the timestamps are recorded in the capture file.

- *Display Raw Timestamp Value* shows the timestamp as the **total time in hundred nanoseconds** from a specific point in time.

- *Display Relative Timestamps* shows the timestamp as the **amount of time that has passed since the first byte was captured**. It works just like a stop watch in that the timestamp for the first byte is 0:00:00.0000 and all subsequent timestamps increment from there. The timestamp is recorded as the actual time, so you can flip back and forth between relative and actual time as needed.

- *Selecting both values* displays the **total time in nanoseconds from the start of the capture** as opposed to a specific point in time.

- *Selecting neither value* displays the **actual chronological time**.

When you select Relative Timestamp, you can set the number of digits to display using the up or down arrows on the numeric list.

18.6.4 Changing the Timestamping Resolution

This option affects the resolution of the timestamp stored in the capture file. The default timestamp is 10 milliseconds. This value is determined by the operating system and is the smallest "normal" resolutions possible.

It is also possible to use "high resolution" timestamping. High resolution timestamp values are marked by an asterisk as high resolution in the drop down list. To change timestamping resolutions:

1. Choose *System Settings* from the *Options* menu on the Control window, and click the *Timestamping Options* button, or click the click the Timestamping Options icon from either the Event Display or Statistics window.

2. Go to the *Capture Options* section of the window.
3. Change the resolution listed in the *Storage Resolution* box. Note that if you change the resolution, you need to exit the analyzer and restart in order for the change to take effect.

18.6.5 Displaying Fractions of a Second

1. Choose *System Settings* from the *Options* menu on the Control window, and click the *Timestamping Options* button, or click the click the Timestamping Options icon from either the Event Display or Statistics window.
2. Go to the *Display Options* section at the bottom of the window, and find the *Number of Digits to Display* box.
3. Click on the arrows to change the number. You can display between 0 and 6 digits to the right of the decimal point.

The options in this section affect only how the timestamps are displayed on the screen, not the resolution used to capture the data.

18.6.6 Converting Timestamps

Serialtest for DOS uses a timebase of Pacific Standard Time during non daylight savings time hours and Pacific Daylight Time during daylight savings time hours. The analyzer always uses Greenwich Mean Time (also known as Universal Time Coordinates).

When importing a Serialtest for DOS file, the analyzer must determine if the file was recorded during daylight savings time or not before converting the timestamps. Because the rules for determining this can change, it is possible for the analyzer to convert the timestamps incorrectly, resulting in timestamps that are off by one hour.

18.6.7 Performance Issues For High Resolution Timestamps

There are two things to be aware of when using high resolution timestamps. The first is that high resolution timestamps take up more space in the capture file because more bits are required to store the timestamp. Also, more timestamps need to be stored than at normal resolutions. The second issue is that using high resolution timestamping may affect performance on slower machines

For example, if 10 bytes of data are captured in 10 milliseconds at a rate of 1 byte per millisecond, and the timestamp resolution is 10 milliseconds, then only one timestamp needs to be stored for the 10 bytes of data. If the resolution is 1 millisecond, then 10 timestamps need to be stored, one for each byte of data. If you have two capture files, both of the same size, but one was captured using normal resolution timestamping and the other using high resolution, the normal resolution file has more data events in it, because less room is used to store timestamps.

You can increase the size of your capture file in the System Settings.

19 Technical Information

19.1 Contacting Technical Support

Technical support is available in several ways. The online help system provides answers to many user related questions. Frontline's website has documentation on common problems, as well as software upgrades and utilities to use with our products.

On the Web: http://www.fte.com/support/default.asp

Email: tech_support@fte.com

If you need to talk to a technical support representative, support is available between 9am and 5pm, U.S. Eastern time, Monday through Friday. Technical support is not available on U.S. national holidays.

Phone: +1 (434) 984-4500

Fax: +1 (434) 984-4505

19.2 Ethernet Performance Notes

As a software-based product, the speed of your computer's processor affects FTS's performance. Receive overrun, frames missed and buffer overflow errors are indicators that FTS is unable to keep up with the data. The information below describes what happens to the data as it arrives at the network card, what the types of errors mean, and how various aspects of FTS affect performance. Also included are suggestions on how to improve performance.

Data captured by the network card first goes into the card's buffer. The card generates an interrupt, which tells the NDIS driver to check the port. The FTS driver takes the data from the NDIS driver and counts each byte as they are put into the FTS driver's buffer. The FTS driver tells the FTS user interface that data is ready to be processed. FTS takes the data from the driver's buffer and puts the data into the capture file.

Receive overruns occur when the frame buffer on the network card is not emptied by the NDIS driver. Frames missed and no buffer errors occur when the FTS driver does not clear out the NDIS driver buffer. In both of these situations, FTS knows that it has lost data, but does not know how much.

Driver Buffer Overflows occur when the FTS user interface does not retrieve frames from the FTS driver quickly enough. The Frames Lost counter on the Statistics window displays the number of frames lost due to driver buffer overflows. Since the driver counts the frames as it retrieves them from the NDIS driver, it not only knows that it has lost data, it also knows how much. Buffer overflows are indicated in the Event Display window by a

plus sign within a circle. Clicking on the buffer overflow symbol displays how many frames have been lost. The Statistics window is a good place to check for buffer overflow errors.

All 3 types of errors indicate that data is coming in too quickly for FTS to process. There are several things that you can do to try and solve this problem.

- Use capture filters to filter out data you don't need to see. Capture filters reduce the amount of data processed by FTS.
- Close all other programs that are doing work while FTS is running. Refrain from doing searches in the Event Display window or other processor intensive activities while FTS is capturing data.
- Timestamping takes up processor time, primarily not in timestamping the data, but in writing the timestamp to the buffer or file. Try turning off timestamping from the Timestamping Options window.
- For Driver Buffer Overflows, change the size of the driver buffer. This value is changed from the Advanced System Settings. Go to the Control Window and choose System Settings from the Options menu. Click on the Advanced button. Find the value Driver Receive Buffer Size in Operating System Pages. Take the number listed there and double it.
- For Frames Missed and No Buffer errors, change the number of NDIS buffers. To do this, choose Hardware Settings from the Options menu on the Control window, and double the value listed in Number of NDIS buffers to use.
- FTS's number one priority is capturing data; updating windows is secondary. However, updating windows still takes a certain amount of processor time, and may cause FTS to lose data while the window is being updated. Some windows require more processing time than others because the information being displayed in them is constantly changing. Refrain from displaying data live in the Event Display and Frame Display windows. Try closing the Statistics windows. FTS can capture data with no windows other than the Control window open.
- If you are still experiencing receive overruns, frames missed errors and/or buffer overflows after trying all of the above options, then you have to use a faster PC.

19.3 Changing Where the Search Lands

When doing a search in the analyzer, the byte or bytes matching the search criteria are highlighted in the Event Display. The first selected byte appears on the third line of the display.

To change the line on which the first selected byte appears:

1. Open fts.ini (located in the C:\Program Files\Common Files\FTE)
2. Go to the [CVEventDisplay] section
3. Change the value for SelectionOffset.
4. If you want the selection to land on the top line of the display, change the SelectionOffset to 0 (zero).

19.4 Progress Bars

The analyzer uses progress bars to indicate the progress of a number of different processes. Some progress bars (such as the filtering progress bar) remain visible, while others are hidden.

The title on the progress bar indicates the process underway.

19.5 Event Numbering

This section talks about how events are numbered when they are first captured and how this affects the display windows in the analyzer. The information in this section applies to frame numbering as well.

When the analyzer captures an *event*, it gives the event a number. If the event is a data byte event, it receives a byte number in addition to an event number. There are usually more events than bytes, with the result is that a byte might be listed as Event 10 of 16 when viewing all events, and Byte 8 of 11 when viewing only the data bytes.

The numbers assigned to events that are *wrapped* out of the buffer are not reassigned. In other words, when event number 1 is wrapped out of the buffer, event number 2 is not renumbered to event 1. This means that the first event in the buffer may be listed as event 11520 of 16334, because events 1-11519 have been wrapped out of the buffer. Since row numbers refer to the event numbers, they work the same way. In the above example, the first row would be listed as 2d00 (which is hex for 11520.)

The advantage of not renumbering events is that you can save a portion of a capture file, send it to a colleague, and tell your colleague to look at a particular event. Since the events are not renumbered, your colleague's file use the same event numbers that your file does.

19.6 Padding of Short Frames

Ethernet requires that frames be a minimum of 60 bytes in length, not including the CRC. If the frame is less than 60 bytes, the NIC pads it before putting it on the wire. Pad characters are usually nulls (hex 00).

Frames transmitted by the PC running the analyzer are looped back by the NDIS driver so the transmitting PC can see the frame. The loopback occurs before the NIC has added any necessary padding to the end of the frame. The analyzer compensates for this by using the sequence "Pad", repeated as many times as necessary, as a placeholder. The analyzer uses only as many characters as needed to bring the frame up to the required 60 bytes, so you may see partial "Pad"s or multiple "Pad"s. For example, you may see "PadPadPad", "PadPa" "Pa", etc.

19.7CRC!

When NDIS receives a frame, it checks that the CRC is good and then discards it before passing the frame up to the next higher layer. The analyzer adds "CRC!" to the end of Ethernet frames to compensate.

NDIS does not pass up frames with bad CRCs, so there is no way for the analyzer to capture them. Some (but not all) NDIS drivers record the number of frames received with bad CRCs. The number of CRC errors is shown in the Errors table on the Statistics window.

To manually determine the CRC for a frame, use the CRC function on the Event Display.

19.8BPF Copyright Notice

This copyright applies to code used in the filter feature. Filtering functionality in FTS is based on Berkeley Packet Filtering (BPF), which is implemented in the UNIX program tcpdump.

Copyright (c) 1990, 1991, 1992, 1993, 1994, 1995, 1996, 1997

The Regents of the University of California. All rights reserved.

This code is derived from the Stanford/CMU enet packet filter, (net/enet.c) distributed as part of 4.3BSD, and code contributed to Berkeley by Steven McCanne and Van Jacobson both of Lawrence Berkeley Laboratory.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- All advertising materials mentioning features or use of this software must display the following acknowledgement: This product includes software developed by the University of California, Berkeley and its contributors.
- Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER

CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

19.9 Useful Character Tables

19.9.1 ASCII Codes

hex	x0	x1	x2	x3	x4	x5	x6	x7	x8	x9	xA	xB	xC	xD	xE	xF
0x	NUL	SOH	STX	ETX	EOT	ENQ	ACK	BEL	BS	HT	LF	VT	FF	CR	SO	SI
1x	DLE	DC1	DC2	DC3	DC4	NAK	SYN	ETB	CAN	EM	SUB	ESC	FS	GS	RS	US
2x	SP	!	"	#	$	%	&	'	(	)	*	+	,	-	.	/
3x	0	1	2	3	4	5	6	7	8	9	:	;	<	=	>	?
4x	@	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
5x	P	Q	R	S	T	U	V	W	X	Y	Z	[	\	]	^	_
6x	`	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
7x	p	q	r	s	t	u	v	w	x	y	z	{	|	}	~	DEL

19.9.2 Baudot Codes

DEC	HEX	LETTERS	FIGURES
0	00	BLANK (NUL)	BLANK (NUL)
1	01	E	3
2	02	LF	LF
3	03	A	-
4	04	SP	SP
5	05	S	BEL
6	06	I	8
7	07	U	7
8	08	CR	CR
9	09	D	$
10	0A	R	4
11	0B	J	'
12	0C	N	,
13	0D	F	!
14	0E	C	:
15	0F	K	(
16	10	T	5
17	11	Z	"
18	12	L	)
19	13	W	2
20	14	H	#
21	15	Y	6
22	16	P	0
23	17	Q	1
24	18	O	9
25	19	B	?
26	1A	G	&
27	1B	FIGURES	FIGURES
28	1C	M	.
29	1D	X	/
30	1E	V	;
31	1F	LETTERS	LETTERS

19.9.3 EBCDIC Codes

hex	x0	x1	x2	x3	x4	x5	x6	x7	x8	x9	xA	xB	xC	xD	xE	xF
0x	NUL	SOH	STX	ETX	PF	HT	LC	DEL			SMM	VT	FF	CR	SO	SI
1x	DLE	DC1	DC2	TM	RES	NL	BS	IL	CAN	EM	CC	CU1	IFS	IGS	IRS	IUS
2x	DS	SOS	FS		BYP	LF	ETB	ESC			SM	CU2		ENQ	ACK	BEL
3x			SYN		PN	RS	UC	EOT				CU3	DC4	NAK		SUB
4x	SP											.	<	(	+	
5x	&										!	$	*	)	;	^
6x	-	/									|	,	%	_	>	?
7x										`	:	#	@	'	=	"
8x		a	b	c	d	e	f	g	h	i						
9x		j	k	l	m	n	o	p	q	r						
Ax		~	s	t	u	v	w	x	y	z				[		
Bx														]		
Cx	{	A	B	C	D	E	F	G	H	I						
Dx	}	J	K	L	M	N	O	P	Q	R						
Ex	\		S	T	U	V	W	X	Y	Z						
Fx	0	1	2	3	4	5	6	7	8	9						

19.9.4 Communication Control Characters

Listed below in alphabetical order are the expanded text meanings for common ANSI communication control characters, and two-character system abbreviation for each one. Some abbreviations have forward slash characters between the two letters. This is to differentiate the abbreviations for a control character from a hex number. For example, the abbreviation for Form Feed is listed as F/F, to differentiate it from the hex number FF.

Abbreviation	Control Character	Text
AK	ACK	Acknowledge
BL	BEL	Bell
BS	BS	Backspace
CN	CAN	Cancel
CR	CR	Carriage Return
D/1-4	DC1-4	Device Control 1-4
D/E	DEL	Delete
DL	DLE	Data Link Escape
EM	EM	End of Medium

EQ	ENQ	Enquiry
ET	EOT	End of Transmission
E/C	ESC	Escape
E/B	ETB	End of Transmission Block
EX	ETX	End of Text
F/F	FF	Form Feed
FS	FS	File Separator
GS	GS	Group Separator
HT	HT	Horizontal Tabulation
LF	LF	Line Feed
NK	NAK	Negative Acknowledge
NU	NUL	Null
RS	RS	Record Separator
SI	SI	Shift In
SO	SO	Shift Out
SH	SOH	Start of Heading
SX	STX	Start of Text
SB	SUB	Substitute
SY	SYN	Synchronous Idle
US	US	Unit

		Separator
VT	VT	Vertical Tabulation

19.10 Frame Decoder

Frame Decoder is for the development of add-on components to extend the functionality of your FTS protocol analyzer. Those add-on components are generally used to decode existing or custom protocols. The core of each such "decoder" is a program that defines how the protocol data are to be broken up into fields and displayed in the Frame Display window of the analyzer software. The DecoderScript Manual provides instruction on how to create custom decoders and use them just like any of the decoders supplied with the protocol analyzer. You can also apply this knowledge to modify decoders supplied with the protocol analyzer.

For more information about Frame Decoder, consult the DecoderScript Manual located in the desktop folder under Optional Components, or simply select *Start | Programs | Frontline [Product Name and Version Number] | Optional Components | DecoderScript Manual*.

20 Index

A

A2DP Decoder Parameters · 10
About Display Filters · 105
Absolute Time · 156
Absolute Timestamp Search · 101
Add a New or Save an Existing Template · 11
Add/Edit an Alias for a Node in Network View · 68
Adding a New Predefined Stack · 18
Adding Comments To A Capture File · 133, 136
Advanced Display Filtering Techniques · 109
Apply Capture Filters · 105, 106, 112, 114, 115, 116, 117, 124
Apply Display Filters · 105, 106, 108, 109, 110, 111, 112
ASCII · 29, 98
  character set · 163
  removing the numbers on the Event Display · 29
  searching for ASCII strings · 98
  viewing data in · 29
ASCII Codes · 163
ASCII Pane · 43
Automatically Request Missing Decoding Information · 21
Auto-Sizing Column Widths · 40
Auto-traversal · 18

B

Bar Charts · 56
Baudot · 29, 149
Baudot Codes · 163
Berkeley Packet Filtering · 115
Binary · 97, 98
Binary Pane · 44
Bookmarks · 103, 104, 127
Boolean · 108, 111, 112
BPF · 115
Buffer · 130
  Buffer Tabs · 55
Byte · 44, 161
  Bytes Per Second Table · 58

C

Calculating Data Rates and Delta Times · 27
Capture Buffer · 130
Capture File · 130, 132, 133, 136
  changing default location of · 154
  loading · 135
  removing framing markers · 21
  saving · 130
Capture Filters · 105, 112, 114, 116, 117, 124
CFA file · 132, 133, 136
Changing Default File Locations · 154
Character · 97, 98
  Character Pane · 43
Character Set · 29, 163, 164
Character Strings in Searching · 98
Characters Per Second Table · 56
Color of Data Bytes · 45
Colors · 45
Column Width · 40
Comma Separated File · 147
Compound Display Filters · 108
Compound Ethernet Capture Filters · 116
Confirm CFA Changes · 132
Context For Decoding · 21
Control Characters · 98
Control Window · 6, 7
  Configuration Information · 5
  Control Window Toolbar · 3
Conversation Capture Filters · 114
Conversation Filters · 109
Copying Statistics · 56
CSV Files · 147
Custom Protocol Stack · 18
Custom Stack · 18
Customizing Fields in the Summary Pane · 40

D

Dashboard
  Dashboard - Define Authorized IP Addresses · 88
  Dashboard - Show IP Addresses Seen · 89
  Network View Dashboard · 81
Data · 27, 129, 130
Data Byte Color Denotation · 45
Data Rates · 27
Decode Pane · 42

Decodes · 21, 33, 42, 95
Default File Locations · 154
Delete a Template · 12
Deleting Display Filters · 110
Delta Times · 27
Difference Between Ethernet Capture Filters · 105
Direction · 109
Directories · 154
Disabling · 156
Display Conversation Information in Network View · 67
Display Filters · 105, 110, 111, 112
Display Options · 158
Dots · 41
Duplicate View · 26, 38

E

Easy Protocol Filtering · 45, 125
EBCDIC · 29
  EBCDIC Codes · 164
Enabling/Disabling Timestamping · 156
Errors · 45, 47, 52, 126, 127
Ethernet Capture Filter · 112, 114, 115, 117, 124
Event Display · 38, 142, 147
  Event Display Export · 147
  Event Display Print · 142
  Event Numbering · 161
  Event Pane · 44
Exclude · 106
Exclude Radio Buttons · 106
Expand All/Collapse All · 42
Expand Decode Pane · 39
Export
  Export Baudot · 149
  Export Events… · 147
  Export Filter Out · 147

F

Field Width · 40
File · 117, 124, 129, 130, 135
File Format Required for Merlin Capture Files · 137
File Locations · 154
Filtering · 46, 68, 115, 125, 127
Filters · 45, 46, 47, 50, 52, 68, 105, 106, 108, 109, 110, 111, 112, 114, 115, 116, 117, 124, 125, 126, 127
Find · 95, 97, 98, 100, 101, 102
Font Size · 32
Fractions Of A Second · 158
Frame Display · 33, 37, 38, 39, 40, 41, 42, 43, 44, 45
  Frame Display Status Bar · 37
  Frame Display Window · 33
  Frame Symbols · 41
Frame Display - Right Click Filtering · 42, 47
Frames Per Second Table · 58
Freeze · 28

G

Graph Refresh Rate · 57
Graphs · 56, 57
Green Dots in Summary Pane · 41

H

Hex · 98
Hexadecimal · 43
Hiding · 50
Hiding Display Filters · 110
Hiding Layers · 51
High Resolution Timestamping · 157, 158

I

Include · 106
Include/Exclude · 106
Information Screen · 18
IP Address
  Filter · 114

L

Layer · 51
Layer Colors · 45
Live Update · 28
Load Filter File · 124

M

MAC Address Filter · 114
Menus · 5
Merlin Files · 137
Minimizing · 7
Mixed Channel/Sides · 30
Mixed Sides Mode · 30
Modify Capture Filters · 114, 117
Modify Display Filters · 111, 112
Multiple Event Displays · 26
Multiple Frame Displays · 38

N

Named Filters · 117, 127
Network View Dashboard · 81
  Define Authorized IP Addresses · 88
  Show IP Addresses Seen · 89
Network View Introduction · 65
Network View Technical Notes · 76
Node Capture Filters · 114
Node Database · 73
Node Filters · 68, 109
Nonprintables · 147
Notes · 133, 136
Numbers · 161

O

Offset · 115
Offset Ethernet Capture Filters · 115
Open · 26, 124
  Open Capture File · 135
Options · 155, 156
Overriding Frame Information · 21

P

Panes · 39
Pattern · 97, 115
Pattern Ethernet Capture Filters · 115
Percentages · 57
Performance Issues For High Resolution Timestamps · 158
Performance Notes · 159
Physical Errors · 45
Pie Charts · 56
Predefined · 115
Predefined Ethernet Capture Filters · 115
Printing · 56, 142
Printing from the Frame Display · 139
Progress Bars · 161
Protocol
  Protocol Layer Colors · 45
Protocol Navigator · 48
Protocol Stack · 18, 19

Q

Quick Export · 147
Quick Filtering · 47, 126

R

Radix · 43
Red Frame Numbers · 45
Relative Time · 100, 156
Relative Timestamp Search · 101
Remove
  Bookmarks · 103
  Columns · 40
  Filters · 110, 114
  Framing Markers · 21
Renaming · 112
Reset Panes · 39
Resetable Tab · 55
Resolution · 157
Resolving DNS Names in Network View · 74
Revealing Display Filters · 110
Revealing Layers · 51
Revealing Protocol Layers · 51

S

Save · 106, 124, 129, 130
Save As · 129
Saving · 124, 129, 130
  Display Filter · 106
Saving the Capture File using File > Save or the Save icon · 129
Search · 95, 97, 98, 100, 101, 102, 104
  binary value · 97
  bookmarks · 104
  character string · 97
  control characters · 98
  entering character strings · 98
  hex or binary characters · 98
  hex pattern · 97
  pattern · 97
  strings in decodes · 95
  timestamp · 100
  wildcards · 97
Set The Count For Top N Filters · 70
Sorting Frames · 38
Start Up Options · 155
Statistics Graphs · 56
Summary Layer Protocol · 46, 125
Summary Pane · 40, 41
Synchronization · 38

T

The Network View Toolbar · 74
Timestamp · 101, 102, 157, 158

Timestamping · 101, 156, 158
Timestamping Options · 156
Timestamping Resolution · 157
Timestamps · 156, 158

U

Unframe · 21
Unframe Function · 21
Unframing · 21
User Defined Stacks · 19
Using BPF · 115
Using Named Filters · 127
Utilization Table · 58

V

Values · 57
Viewing Data Events · 28